Calendar No. 673

114TH CONGRESS
2D SESSION

S. 1869

[Report No. 114–378]

To improve Federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian Federal networks.

IN THE SENATE OF THE UNITED STATES

JULY 27, 2015

Mr. CARPER (for himself and Mr. JOHNSON) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

NOVEMBER 17, 2016

Reported by Mr. JOHNSON, with amendments

[Omit the part struck through and insert the part printed in italic]

A BILL

To improve Federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian Federal networks.

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 Cybersecurity Enhancement Act of 2015''~~ *''Federal Cybersecurity Enhancement Act of 2016''*.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 3(a);

(3) the term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 3(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(7) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 3. IMPROVED FEDERAL NETWORK SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

''SEC. 228. CYBERSECURITY PLANS.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an

agency, by a contractor of an agency, or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227; *and*

~~''(3) the term 'information sharing and analysis organization' has the meaning given the term in section 212(5); and~~

''(4*3*) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

"SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

"(a) DEFINITIONS.—In this section—

"(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

"(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

"(3) the term 'agency information system' has the meaning given the term in section 228; and

"(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

"(b) REQUIREMENT.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

"(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity

providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); ~~and~~

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note)~~.~~*; and*

"(7) shall ensure that—

"(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

"(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

"(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

"(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

"(d) PRIVATE ENTITIES.—

"(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

"(A) disclose any network traffic transiting or traveling to or from an agency information

system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the pro-

gram carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.".

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency in-

formation system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

"Sec. 226. Cybersecurity recruitment and retention.
"Sec. 227. National cybersecurity and communications integration center.
"Sec. 228. Cybersecurity plans.
"Sec. 229. Clearances.
"Sec. 230. Federal intrusion detection and prevention system.".

SEC. 4. ADVANCED INTERNAL DEFENSES.

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting ‘‘, operating, and maintaining’’ after ‘‘deploying’’.

SEC. 5. FEDERAL CYBERSECURITY BEST PRACTICES.

(a) ASSESSMENT OF BEST PRACTICES FOR FEDERAL CYBERSECURITY.—The Secretary, in consultation with the Director, shall regularly assess and require implementation of best practices for securing agency information systems against intrusion and preventing data exfiltration in the event of an intrusion.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), not later than 1 year after the date of enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for read-

ily accessible storage of the data, and individuals' need to access the data;

(C) encrypt the data described in subparagraph (A) that is stored on or transiting agency information systems consistent with standards and guidelines promulgated under section 11331 of title 40, United States Code;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement multi-factor authentication consistent with standards and guidelines promulgated under section 11331 of title 40, United States Code, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.

SEC. 6. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 3(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 3(a) of this Act.

(b) THIRD-PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the

date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency

information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; ~~and~~

(vi) an explanation of whether any information on individuals, and to the greatest extent practicable, on United States persons, whose personally identifiable information is not necessary to describe a cybersecurity risk has been retained incidentally under the intrusion detection and prevention capabilities, and if such information has been retained, for what purpose and for what length of time; and

(~~vi~~*vii*) a description of the pilot established under section 230(c)(5) of the

Homeland Security Act of 2002, as added by section 3(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and

techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report re-

quired under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 4(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 5(a); and

(v) a list by agency of compliance with the requirements of section 5(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 4(a)(2); and

(ii) the improved metrics developed pursuant to section 4(b).

SEC. 7. TERMINATION.

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 3(a) of this Act, and the reporting requirements under section 6(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 3(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 8. IDENTIFICATION OF UNCLASSIFIED INFORMATION SYSTEMS.

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that, when combined with other unclassified information, may comprise classified information;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently classified; and

(2) the Director of National Intelligence shall submit to the appropriate congressional committees a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, but may include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense or an element of the intelligence community.

SEC. 9. OPM DATA BREACH DAMAGE ASSESSMENT.

(a) ASSESSMENT.—The Secretary and the Director of National Intelligence shall jointly, and in coordination with the head of each appropriate agency, conduct an ongoing damage and risk assessment relating to the data breaches at the Office of Personnel Management (referred to in this section as the "OPM data breach").

(b) REPORTS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and once not later than 180 days thereafter, the Director of National Intelligence shall submit to Congress a report on the assessment conducted under subsection (a).

(2) CONTENTS.—Each report submitted under this subsection shall include—

(A) updates on the extent to which Federal data was compromised, exfiltrated, or manipulated by the same entity that caused the OPM data breach;

(B) analysis of the impact of the OPM data breach on national security; and

(C) analysis of whether any information accessed through the OPM data breach has been released or deployed, whether publicly or privately.

(3) UNCLASSIFIED FORM.—Each report submitted under this subsection shall be in unclassified form, but may include a classified annex.

SEC. 10. DIRECTION TO AGENCIES.

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

"(h) 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, 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;

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

"(E) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

"(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) NOTICE.—The Secretary shall immediately notify the Director, the head and chief information officer (or equivalent official) of each agency to which specific actions were taken pursuant to subparagraph (A), and the appropriate congressional committees and authorizing committees of each such agencies of—

"(i) any action taken under subparagraph (A); and

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

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

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

"(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.

"(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the

appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

"(j) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term 'appropriate congressional committees' means—

"(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(2) the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.".

Calendar No. 673

114TH CONGRESS
2D SESSION

S. 1869

[Report No. 114–378]

A BILL

To improve Federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian Federal networks.

NOVEMBER 17, 2016

Reported with amendments