Calendar No. 564

113TH CONGRESS
2D SESSION

S. 2521

[Report No. 113–256]

To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

IN THE SENATE OF THE UNITED STATES

JUNE 24, 2014

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

SEPTEMBER 15, 2014

Reported by Mr. CARPER, without amendment

A BILL

To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

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 Modernization Act of 2014''.

SEC. 2. FISMA REFORM.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are to—

''(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

''(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

''(4) provide a mechanism for improved oversight of Federal agency information security programs;

''(5) acknowledge that commercially developed information security products offer advanced, dy-

namic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

''(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

"§ 3552. Definitions

''(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

''(1) The term 'binding operational directive' means a compulsory direction to an agency that is in accordance with policies, principles, standards, and guidelines issued by the Director.

''(2) The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, con-

fidentiality, or availability of information or an information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

''(3) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, which means ensuring timely and reliable access to and use of information.

''(4) The term 'information technology' has the meaning given that term in section 11101 of title 40.

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

''(6)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be

kept classified in the interest of national defense or foreign policy.

''(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

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

''§ 3553. Authority and functions of the Director and the Secretary

''(a) DIRECTOR.—The Director shall oversee agency information security policies, including—

''(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

''(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

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

''(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

''(4) 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;

''(5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

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

''(7) consulting with the Secretary in carrying out the authorities and functions under this subsection.

''(b) SECRETARY.—The Secretary, in consultation with the Director, shall oversee the operational aspects of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

''(1) assisting the Director in carrying out the authorities and functions under subsection (a);

''(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

''(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

"(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

"(C) requirements for the mitigation of exigent risks to information systems; and

"(D) other operational requirements as the Director or Secretary may determine necessary;

"(3) monitoring agency implementation of information security policies and practices;

"(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

"(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603;

"(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

"(A) operating the Federal information security incident center established under section 3556;

''(B) upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

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

''(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems; and

''(7) other actions as the Secretary may determine necessary to carry out this subsection on behalf of the Director.

''(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

''(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

''(2) a description of the threshold for reporting major information security incidents;

''(3) a summary of the results of evaluations required to be performed under section 3555;

''(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

''(5) an assessment of agency compliance with the policies and procedures established under section 3559(a).

''(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(4) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

''(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

''(2) 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) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

''§ 3554. Federal agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

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

''(ii) information systems used or operated by an agency or by a contractor of

an agency or other organization on behalf of an agency;

''(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

''(i) information security standards promulgated under section 11331 of title 40;

''(ii) operational directives developed by the Secretary under section 3553(b);

''(iii) policies and procedures issued by the Director under section 3559; and

''(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

''(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

''(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

''(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

''(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

''(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

''(A) designating a senior agency information security officer who shall—

"(i) carry out the Chief Information Officer's responsibilities under this section;

"(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

"(iii) have information security duties as that official's primary duty; and

"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

"(B) developing and maintaining an agency-wide information security program as required by subsection (b);

"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

''(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

''(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

''(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

''(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

''(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

''(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided

or managed by another agency, contractor, or other source, that includes—

''(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

''(2) policies and procedures that—

''(A) are based on the risk assessments required by paragraph (1);

''(B) cost-effectively reduce information security risks to an acceptable level;

''(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

''(D) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

''(iii) minimally acceptable system configuration requirements, as determined by the agency; and

''(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

''(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

''(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

''(A) information security risks associated with their activities; and

''(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

''(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a fre-

quency depending on risk, but no less than annually, of which such testing—

''(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

''(B) may include testing relied on in an evaluation under section 3555;

''(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

''(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines described in section 3556(b), including—

''(A) mitigating risks associated with such incidents before substantial damage is done;

''(B) notifying and consulting with the Federal information security incident center established in section 3556; and

''(C) notifying and consulting with, as appropriate—

''(i) law enforcement agencies and relevant Offices of Inspector General;

''(ii) an office designated by the President for any incident involving a national security system;

''(iii) the committees of Congress described in subsection (c)(1)—

''(I) not later than 7 days after the date on which the incident is discovered; and

''(II) after the initial notification under subclause (I), within a reasonable period of time after additional information relating to the incident is discovered; and

''(iv) any other agency or office, in accordance with law or as directed by the President; and

''(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

''(c) AGENCY REPORTING.—

''(1) ANNUAL REPORT.—

''(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on

Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

''(i) a description of each major information security incident or related sets of incidents, including summaries of—

''(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

''(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred; and

''(III) the detection, response, and remediation actions;

''(ii) the total number of information security incidents, including a description of incidents resulting in significant com-

promise of information security, system impact levels, types of incident, and locations of affected systems;

''(iii) a description of each major information security incident that involved a breach of personally identifiable information, including—

''(I) the number of individuals whose information was affected by the major information security incident; and

''(II) a description of the information that was breached or exposed; and

''(iv) any other information as the Secretary may require.

''(B) UNCLASSIFIED REPORT.—

''(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

''(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the

reports submitted by the agency under subparagraph (A).

''(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

''(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

''(A) the time periods; and

''(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

''(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

''(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"§ 3555. Annual independent evaluation

''(a) IN GENERAL.—(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

''(2) Each evaluation under this section shall include—

''(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

''(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

''(C) separate presentations, as appropriate, regarding information security relating to national security systems.

''(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

''(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

''(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

''(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

''(1) only by an entity designated by the agency head; and

''(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

''(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

''(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

''(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

''(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

''(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

''(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

''(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intel-

ligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

''(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

''(1) the adequacy and effectiveness of agency information security policies and practices; and

''(2) implementation of the requirements of this subchapter.

''(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

''§ 3556. Federal information security incident center

''(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to—

''(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

''(2) compile and analyze information about incidents that threaten information security;

''(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;

''(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

''(5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

''(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

"§ 3557. National security systems

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

''(3) complies with the requirements of this subchapter.

"§ 3558. Effect on existing law

''Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the man-

agement and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code is amended by striking the matter relating to subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''3551. Purposes.
''3552. Definitions.
''3553. Authority and functions of the Director and the Secretary.
''3554. Federal agency responsibilities.
''3555. Annual independent evaluation.
''3556. Federal information security incident center.
''3557. National security systems.
''3558. Effect on existing law.''.

(2) CYBERSECURITY RESEARCH AND DEVELOPMENT ACT.—Section 8(d)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7406) is amended by striking ''section 3534'' and inserting ''section 3554''.

(3) HOMELAND SECURITY ACT OF 2002.—Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511) by striking ''section 3532(3)'' and inserting ''section 3552(b)(5)''.

(4) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT.—Section 20 of the National In-

stitute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(A) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)(5)''; and

(B) in subsection (e)—

(i) in paragraph (2), by striking ''section 3532(1)'' and inserting ''section 3552(b)(2)''; and

(ii) in paragraph (5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)(5)''.

(5) TITLE 10.—Title 10, United States Code, is amended—

(A) in section 2222(j)(5), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)(5)'';

(B) in section 2223(c)(3), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)(5)''; and

(C) in section 2315, by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)(5)''.

(c) OTHER PROVISIONS.—

(1) CIRCULAR A-130.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall revise Office of Management and Budget Circular A–130 to eliminate inefficient or wasteful reporting.

(2) ISPAB.—Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(A) in paragraph (2), by inserting ", the Secretary of Homeland Security," after "the Institute"; and

(B) in paragraph (3), by inserting "the Secretary of Homeland Security," after "the Secretary of Commerce,".

SEC. 3. FEDERAL DATA BREACH RESPONSE GUIDELINES.

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, as added by this Act, is amended by adding at the end the following:

"§ 3559. Privacy breach requirements

"(a) POLICIES AND PROCEDURES.—The Director, in consultation with the Secretary, shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

''(1) timely notice to affected individuals based on a determination of the level of risk and consistent with law enforcement and national security considerations;

''(2) timely reporting to the Federal information security incident center established under section 3556 or other Federal cybersecurity center, as designated by the Director;

''(3) timely notice to committees of Congress with jurisdiction over cybersecurity; and

''(4) such additional actions as the Director may determine necessary and appropriate, including the provision of risk mitigation measures to affected individuals.

''(b) CONSIDERATIONS.—In carrying out subsection (a), the Director shall consider recommendations made by the Government Accountability Office, including recommendations in the December 2013 Government Accountability Office report entitled 'Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent' (GAO–14–34).

''(c) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or

control of the agency comply with policies and procedures established under subsection (a).

''(d) TIMELINESS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the policies and procedures established under subsection (a) shall require that the notice to affected individuals required under subsection (a)(1) be made without unreasonable delay and with consideration of the likely risk of harm and the level of impact, but not later than 60 days after the date on which the head of an agency discovers the breach of information security involving the disclosure of personally identifiable information.

''(2) DELAY.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary may delay the notice to affected individuals under subsection (a)(1) for not more than 180 days, if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions from the breach of information security involving the disclosure of personally identifiable information.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subchapter II for chapter 35 of title 44, United States Code, as added by this Act, is amended by inserting after the item relating to section 3558 the following:

"3559. Privacy breach requirements.".

Calendar No. 564

113TH CONGRESS
2D SESSION

S. 2521

[Report No. 113–256]

A BILL

To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

SEPTEMBER 15, 2014

Reported without amendment