

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Information
5 Security Modernization Act of 2014”.

1 **SEC. 2. FISMA REFORM.**

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

5 “SUBCHAPTER II—INFORMATION SECURITY

6 “§ 3551. **Purposes**

7 “The purposes of this subchapter are to—

8 “(1) provide a comprehensive framework for en-
9 suring the effectiveness of information security con-
10 trols over information resources that support Fed-
11 eral operations and assets;

12 “(2) recognize the highly networked nature of
13 the current Federal computing environment and pro-
14 vide effective governmentwide management and over-
15 sight of the related information security risks, in-
16 cluding coordination of information security efforts
17 throughout the civilian, national security, and law
18 enforcement communities;

19 “(3) provide for development and maintenance
20 of minimum controls required to protect Federal in-
21 formation and information systems;

22 “(4) provide a mechanism for improved over-
23 sight of Federal agency information security pro-
24 grams;

25 “(5) acknowledge that commercially developed
26 information security products offer advanced, dy-

1 namic, robust, and effective information security so-
2 lutions, reflecting market solutions for the protection
3 of critical information infrastructures important to
4 the national defense and economic security of the
5 nation that are designed, built, and operated by the
6 private sector; and

7 “(6) recognize that the selection of specific
8 technical hardware and software information secu-
9 rity solutions should be left to individual agencies
10 from among commercially developed products.

11 **“§ 3552. Definitions**

12 “(a) IN GENERAL.—Except as provided under sub-
13 section (b), the definitions under section 3502 shall apply
14 to this subchapter.

15 “(b) ADDITIONAL DEFINITIONS.—As used in this
16 subchapter:

17 “(1) The term ‘binding operational directive’
18 means a compulsory direction to an agency that is
19 in accordance with policies, principles, standards,
20 and guidelines issued by the Director.

21 “(2) The term ‘incident’ means an occurrence
22 that—

23 “(A) actually or imminently jeopardizes,
24 without lawful authority, the integrity, con-

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

3 “(B) constitutes a violation or imminent
4 threat of violation of law, security policies, secu-
5 rity procedures, or acceptable use policies.

6 “(3) The term ‘information security’ means
7 protecting information and information systems
8 from unauthorized access, use, disclosure, disrup-
9 tion, modification, or destruction in order to pro-
10 vide—

11 “(A) integrity, which means guarding
12 against improper information modification or
13 destruction, and includes ensuring information
14 nonrepudiation and authenticity;

15 “(B) confidentiality, which means pre-
16 serving authorized restrictions on access and
17 disclosure, including means for protecting per-
18 sonal privacy and proprietary information; and

19 “(C) availability, which means ensuring
20 timely and reliable access to and use of infor-
21 mation.

22 “(4) The term ‘information technology’ has the
23 meaning given that term in section 11101 of title
24 40.

1 “(5) The term ‘intelligence community’ has the
2 meaning given that term in section 3(4) of the Na-
3 tional Security Act of 1947 (50 U.S.C. 3003(4)).

4 “(6)(A) The term ‘national security system’
5 means any information system (including any tele-
6 communications system) used or operated by an
7 agency or by a contractor of an agency, or other or-
8 ganization on behalf of an agency—

9 “(i) the function, operation, or use of
10 which—

11 “(I) involves intelligence activities;

12 “(II) involves cryptologic activities re-
13 lated to national security;

14 “(III) involves command and control
15 of military forces;

16 “(IV) involves equipment that is an
17 integral part of a weapon or weapons sys-
18 tem; or

19 “(V) subject to subparagraph (B), is
20 critical to the direct fulfillment of military
21 or intelligence missions; or

22 “(ii) is protected at all times by procedures
23 established for information that have been spe-
24 cifically authorized under criteria established by
25 an Executive order or an Act of Congress to be

1 kept classified in the interest of national de-
2 fense or foreign policy.

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

7 “(7) The term ‘Secretary’ means the Secretary
8 of Homeland Security.

9 **“§ 3553. Authority and functions of the Director and**
10 **the Secretary**

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

13 “(1) developing and overseeing the implementa-
14 tion of policies, principles, standards, and guidelines
15 on information security, including through ensuring
16 timely agency adoption of and compliance with
17 standards promulgated under section 11331 of title
18 40;

19 “(2) requiring agencies, consistent with the
20 standards promulgated under such section 11331
21 and the requirements of this subchapter, to identify
22 and provide information security protections com-
23 mensurate with the risk and magnitude of the harm
24 resulting from the unauthorized access, use, dislo-
25 sure, disruption, modification, or destruction of—

1 “(A) information collected or maintained
2 by or on behalf of an agency; or

3 “(B) information systems used or operated
4 by an agency or by a contractor of an agency
5 or other organization on behalf of an agency;

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

8 “(4) coordinating the development of standards
9 and guidelines under section 20 of the National In-
10 stitute of Standards and Technology Act (15 U.S.C.
11 278g-3) with agencies and offices operating or exer-
12 cising control of national security systems (including
13 the National Security Agency) to assure, to the max-
14 imum extent feasible, that such standards and
15 guidelines are complementary with standards and
16 guidelines developed for national security systems;

17 “(5) overseeing agency compliance with the re-
18 quirements of this subchapter, including through
19 any authorized action under section 11303 of title
20 40, to enforce accountability for compliance with
21 such requirements;

22 “(6) coordinating information security policies
23 and procedures with related information resources
24 management policies and procedures; and

1 “(7) consulting with the Secretary in carrying
2 out the authorities and functions under this sub-
3 section.

4 “(b) SECRETARY.—The Secretary, in consultation
5 with the Director, shall oversee the operational aspects of
6 agency information security policies and practices for in-
7 formation systems, except for national security systems
8 and information systems described in paragraph (2) or (3)
9 of subsection (e), including—

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

12 “(2) developing and overseeing the implementa-
13 tion of binding operational directives to agencies to
14 implement the policies, principles, standards, and
15 guidelines developed by the Director under sub-
16 section (a)(1) and the requirements of this sub-
17 chapter, which may be repealed by the Director if
18 the operational directives issued on behalf of the Di-
19 rector are not in accordance with policies, principles,
20 standards, and guidelines developed by the Director,
21 including—

22 “(A) requirements for reporting security
23 incidents to the Federal information security in-
24 cident center established under section 3556;

1 “(B) requirements for the contents of the
2 annual reports required to be submitted under
3 section 3554(e)(1);

4 “(C) requirements for the mitigation of ex-
5 igent risks to information systems; and

6 “(D) other operational requirements as the
7 Director or Secretary may determine necessary;

8 “(3) monitoring agency implementation of in-
9 formation security policies and practices;

10 “(4) convening meetings with senior agency of-
11 ficials to help ensure effective implementation of in-
12 formation security policies and practices;

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

17 “(6) providing operational and technical assist-
18 ance to agencies in implementing policies, principles,
19 standards, and guidelines on information security,
20 including implementation of standards promulgated
21 under section 11331 of title 40, including by—

22 “(A) operating the Federal information se-
23 curity incident center established under section
24 3556;

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

5 “(C) compiling and analyzing data on
6 agency information security; and

7 “(D) developing and conducting targeted
8 operational evaluations, including threat and
9 vulnerability assessments, on the information
10 systems; and

11 “(7) other actions as the Secretary may deter-
12 mine necessary to carry out this subsection on behalf
13 of the Director.

14 “(c) REPORT.—Not later than March 1 of each year,
15 the Director, in consultation with the Secretary, shall sub-
16 mit to Congress a report on the effectiveness of informa-
17 tion security policies and practices during the preceding
18 year, including—

19 “(1) a summary of the incidents described in
20 the annual reports required to be submitted under
21 section 3554(c)(1), including a summary of the in-
22 formation required under section 3554(c)(1)(A)(iii);

23 “(2) a description of the threshold for reporting
24 major information security incidents;

1 “(3) a summary of the results of evaluations re-
2 quired to be performed under section 3555;

3 “(4) an assessment of agency compliance with
4 standards promulgated under section 11331 of title
5 40; and

6 “(5) an assessment of agency compliance with
7 the policies and procedures established under section
8 3559(a).

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

14 “(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE
15 COMMUNITY SYSTEMS.—(1) The authorities of the Direc-
16 tor described in paragraphs (1) and (2) of subsection (a)
17 shall be delegated to the Secretary of Defense in the case
18 of systems described in paragraph (2) and to the Director
19 of National Intelligence in the case of systems described
20 in paragraph (3).

21 “(2) The systems described in this paragraph are sys-
22 tems that are operated by the Department of Defense, a
23 contractor of the Department of Defense, or another enti-
24 ty on behalf of the Department of Defense that processes
25 any information the unauthorized access, use, disclosure,

1 disruption, modification, or destruction of which would
2 have a debilitating impact on the mission of the Depart-
3 ment of Defense.

4 “(3) The systems described in this paragraph are sys-
5 tems that are operated by an element of the intelligence
6 community, a contractor of an element of the intelligence
7 community, or another entity on behalf of an element of
8 the intelligence community that processes any information
9 the unauthorized access, use, disclosure, disruption, modi-
10 fication, or destruction of which would have a debilitating
11 impact on the mission of an element of the intelligence
12 community.

13 **“§ 3554. Federal agency responsibilities**

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

15 “(1) be responsible for—

16 “(A) providing information security protec-
17 tions commensurate with the risk and mag-
18 nitude of the harm resulting from unauthorized
19 access, use, disclosure, disruption, modification,
20 or destruction of—

21 “(i) information collected or main-
22 tained by or on behalf of the agency; and

23 “(ii) information systems used or op-
24 erated by an agency or by a contractor of

1 an agency or other organization on behalf
2 of an agency;

3 “(B) complying with the requirements of
4 this subchapter and related policies, procedures,
5 standards, and guidelines, including—

6 “(i) information security standards
7 promulgated under section 11331 of title
8 40;

9 “(ii) operational directives developed
10 by the Secretary under section 3553(b);

11 “(iii) policies and procedures issued
12 by the Director under section 3559; and

13 “(iv) information security standards
14 and guidelines for national security sys-
15 tems issued in accordance with law and as
16 directed by the President; and

17 “(C) ensuring that information security
18 management processes are integrated with
19 agency strategic and operational planning pro-
20 cesses;

21 “(2) ensure that senior agency officials provide
22 information security for the information and infor-
23 mation systems that support the operations and as-
24 sets under their control, including through—

1 “(A) assessing the risk and magnitude of
2 the harm that could result from the unauthor-
3 ized access, use, disclosure, disruption, modi-
4 fication, or destruction of such information or
5 information systems;

6 “(B) determining the levels of information
7 security appropriate to protect such information
8 and information systems in accordance with
9 standards promulgated under section 11331 of
10 title 40, for information security classifications
11 and related requirements;

12 “(C) implementing policies and procedures
13 to cost-effectively reduce risks to an acceptable
14 level; and

15 “(D) periodically testing and evaluating in-
16 formation security controls and techniques to
17 ensure that they are effectively implemented;

18 “(3) delegate to the agency Chief Information
19 Officer established under section 3506 (or com-
20 parable official in an agency not covered by such
21 section) the authority to ensure compliance with the
22 requirements imposed on the agency under this sub-
23 chapter, including—

24 “(A) designating a senior agency informa-
25 tion security officer who shall—

1 “(i) carry out the Chief Information
2 Officer’s responsibilities under this section;

3 “(ii) possess professional qualifica-
4 tions, including training and experience,
5 required to administer the functions de-
6 scribed under this section;

7 “(iii) have information security duties
8 as that official’s primary duty; and

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

12 “(B) developing and maintaining an agen-
13 cy-wide information security program as re-
14 quired by subsection (b);

15 “(C) developing and maintaining informa-
16 tion security policies, procedures, and control
17 techniques to address all applicable require-
18 ments, including those issued under section
19 3553 of this title and section 11331 of title 40;

20 “(D) training and overseeing personnel
21 with significant responsibilities for information
22 security with respect to such responsibilities;
23 and

1 “(E) assisting senior agency officials con-
2 cerning their responsibilities under paragraph
3 (2);

4 “(4) ensure that the agency has trained per-
5 sonnel sufficient to assist the agency in complying
6 with the requirements of this subchapter and related
7 policies, procedures, standards, and guidelines;

8 “(5) ensure that the agency Chief Information
9 Officer, in coordination with other senior agency of-
10 ficials, reports annually to the agency head on the
11 effectiveness of the agency information security pro-
12 gram, including progress of remedial actions;

13 “(6) ensure that senior agency officials, includ-
14 ing chief information officers of component agencies
15 or equivalent officials, carry out responsibilities
16 under this subchapter as directed by the official del-
17 egated authority under paragraph (3); and

18 “(7) ensure that all personnel are held account-
19 able for complying with the agency-wide information
20 security program implemented under subsection (b).

21 “(b) AGENCY PROGRAM.—Each agency shall develop,
22 document, and implement an agency-wide information se-
23 curity program to provide information security for the in-
24 formation and information systems that support the oper-
25 ations and assets of the agency, including those provided

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

3 “(1) periodic assessments of the risk and mag-
4 nitude of the harm that could result from the unau-
5 thorized access, use, disclosure, disruption, modifica-
6 tion, or destruction of information and information
7 systems that support the operations and assets of
8 the agency;

9 “(2) policies and procedures that—

10 “(A) are based on the risk assessments re-
11 quired by paragraph (1);

12 “(B) cost-effectively reduce information se-
13 curity risks to an acceptable level;

14 “(C) ensure that information security is
15 addressed throughout the life cycle of each
16 agency information system; and

17 “(D) ensure compliance with—

18 “(i) the requirements of this sub-
19 chapter;

20 “(ii) policies and procedures as may
21 be prescribed by the Director, and infor-
22 mation security standards promulgated
23 under section 11331 of title 40;

1 “(iii) minimally acceptable system
2 configuration requirements, as determined
3 by the agency; and

4 “(iv) any other applicable require-
5 ments, including standards and guidelines
6 for national security systems issued in ac-
7 cordance with law and as directed by the
8 President;

9 “(3) subordinate plans for providing adequate
10 information security for networks, facilities, and sys-
11 tems or groups of information systems, as appro-
12 priate;

13 “(4) security awareness training to inform per-
14 sonnel, including contractors and other users of in-
15 formation systems that support the operations and
16 assets of the agency, of—

17 “(A) information security risks associated
18 with their activities; and

19 “(B) their responsibilities in complying
20 with agency policies and procedures designed to
21 reduce these risks;

22 “(5) periodic testing and evaluation of the ef-
23 fectiveness of information security policies, proce-
24 dures, and practices, to be performed with a fre-

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

3 “(A) shall include testing of management,
4 operational, and technical controls of every in-
5 formation system identified in the inventory re-
6 quired under section 3505(c); and

7 “(B) may include testing relied on in an
8 evaluation under section 3555;

9 “(6) a process for planning, implementing, eval-
10 uating, and documenting remedial action to address
11 any deficiencies in the information security policies,
12 procedures, and practices of the agency;

13 “(7) procedures for detecting, reporting, and re-
14 sponding to security incidents, consistent with stand-
15 ards and guidelines described in section 3556(b), in-
16 cluding—

17 “(A) mitigating risks associated with such
18 incidents before substantial damage is done;

19 “(B) notifying and consulting with the
20 Federal information security incident center es-
21 tablished in section 3556; and

22 “(C) notifying and consulting with, as ap-
23 propriate—

24 “(i) law enforcement agencies and rel-
25 evant Offices of Inspector General;

1 “(ii) an office designated by the Presi-
2 dent for any incident involving a national
3 security system;

4 “(iii) the committees of Congress de-
5 scribed in subsection (c)(1)—

6 “(I) not later than 7 days after
7 the date on which the incident is dis-
8 covered; and

9 “(II) after the initial notification
10 under subclause (I), within a reason-
11 able period of time after additional in-
12 formation relating to the incident is
13 discovered; and

14 “(iv) any other agency or office, in ac-
15 cordance with law or as directed by the
16 President; and

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

20 “(c) AGENCY REPORTING.—

21 “(1) ANNUAL REPORT.—

22 “(A) IN GENERAL.—Each agency shall
23 submit to the Director, the Secretary, the Com-
24 mittee on Government Reform, the Committee
25 on Homeland Security, and the Committee on

1 Science of the House of Representatives, the
2 Committee on Homeland Security and Govern-
3 mental Affairs and the Committee on Com-
4 merce, Science, and Transportation of the Sen-
5 ate, the appropriate authorization and appro-
6 priations committees of Congress, and the
7 Comptroller General a report on the adequacy
8 and effectiveness of information security poli-
9 cies, procedures, and practices, including—

10 “(i) a description of each major infor-
11 mation security incident or related sets of
12 incidents, including summaries of—

13 “(I) the threats and threat ac-
14 tors, vulnerabilities, and impacts re-
15 lating to the incident;

16 “(II) the risk assessments con-
17 ducted under section 3554(a)(2)(A) of
18 the affected information systems be-
19 fore the date on which the incident oc-
20 curred; and

21 “(III) the detection, response,
22 and remediation actions;

23 “(ii) the total number of information
24 security incidents, including a description
25 of incidents resulting in significant com-

1 promise of information security, system
2 impact levels, types of incident, and loca-
3 tions of affected systems;

4 “(iii) a description of each major in-
5 formation security incident that involved a
6 breach of personally identifiable informa-
7 tion, including—

8 “(I) the number of individuals
9 whose information was affected by the
10 major information security incident;
11 and

12 “(II) a description of the infor-
13 mation that was breached or exposed;
14 and

15 “(iv) any other information as the
16 Secretary may require.

17 “(B) UNCLASSIFIED REPORT.—

18 “(i) IN GENERAL.—Each report sub-
19 mitted under subparagraph (A) shall be in
20 unclassified form, but may include a classi-
21 fied annex.

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

1 reports submitted by the agency under
2 subparagraph (A).

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

7 “(d) PERFORMANCE PLAN.—(1) In addition to the
8 requirements of subsection (c), each agency, in consulta-
9 tion with the Director, shall include as part of the per-
10 formance plan required under section 1115 of title 31 a
11 description of—

12 “(A) the time periods; and

13 “(B) the resources, including budget, staffing,
14 and training,

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

17 “(2) The description under paragraph (1) shall be
18 based on the risk assessments required under subsection
19 (b)(1).

20 “(e) PUBLIC NOTICE AND COMMENT.—Each agency
21 shall provide the public with timely notice and opportuni-
22 ties for comment on proposed information security policies
23 and procedures to the extent that such policies and proce-
24 dures affect communication with the public.

1 **“§ 3555. Annual independent evaluation**

2 “(a) IN GENERAL.—(1) Each year each agency shall
3 have performed an independent evaluation of the informa-
4 tion security program and practices of that agency to de-
5 termine the effectiveness of such program and practices.

6 “(2) Each evaluation under this section shall in-
7 clude—

8 “(A) testing of the effectiveness of information
9 security policies, procedures, and practices of a rep-
10 resentative subset of the agency’s information sys-
11 tems;

12 “(B) an assessment of the effectiveness of the
13 information security policies, procedures, and prac-
14 tices of the agency; and

15 “(C) separate presentations, as appropriate, re-
16 garding information security relating to national se-
17 curity systems.

18 “(b) INDEPENDENT AUDITOR.—Subject to sub-
19 section (c)—

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

1 “(2) for each agency to which paragraph (1)
2 does not apply, the head of the agency shall engage
3 an independent external auditor to perform the eval-
4 uation.

5 “(c) NATIONAL SECURITY SYSTEMS.—For each
6 agency operating or exercising control of a national secu-
7 rity system, that portion of the evaluation required by this
8 section directly relating to a national security system shall
9 be performed—

10 “(1) only by an entity designated by the agency
11 head; and

12 “(2) in such a manner as to ensure appropriate
13 protection for information associated with any infor-
14 mation security vulnerability in such system com-
15 mensurate with the risk and in accordance with all
16 applicable laws.

17 “(d) EXISTING EVALUATIONS.—The evaluation re-
18 quired by this section may be based in whole or in part
19 on an audit, evaluation, or report relating to programs or
20 practices of the applicable agency.

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

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

6 “(f) PROTECTION OF INFORMATION.—Agencies and
7 evaluators shall take appropriate steps to ensure the pro-
8 tection of information which, if disclosed, may adversely
9 affect information security. Such protections shall be com-
10 mensurate with the risk and comply with all applicable
11 laws and regulations.

12 “(g) OMB REPORTS TO CONGRESS.—(1) The Direc-
13 tor shall summarize the results of the evaluations con-
14 ducted under this section in the report to Congress re-
15 quired under section 3553(c).

16 “(2) The Director’s report to Congress under this
17 subsection shall summarize information regarding infor-
18 mation security relating to national security systems in
19 such a manner as to ensure appropriate protection for in-
20 formation associated with any information security vulner-
21 ability in such system commensurate with the risk and in
22 accordance with all applicable laws.

23 “(3) Evaluations and any other descriptions of infor-
24 mation systems under the authority and control of the Di-
25 rector of Central Intelligence or of National Foreign Intel-

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

5 “(h) COMPTROLLER GENERAL.—The Comptroller
6 General shall periodically evaluate and report to Congress
7 on—

8 “(1) the adequacy and effectiveness of agency
9 information security policies and practices; and

10 “(2) implementation of the requirements of this
11 subchapter.

12 “(i) ASSESSMENT TECHNICAL ASSISTANCE.—The
13 Comptroller General may provide technical assistance to
14 an Inspector General or the head of an agency, as applica-
15 ble, to assist the Inspector General or head of an agency
16 in carrying out the duties under this section, including by
17 testing information security controls and procedures.

18 **“§ 3556. Federal information security incident center**

19 “(a) IN GENERAL.—The Secretary shall ensure the
20 operation of a central Federal information security inci-
21 dent center to—

22 “(1) provide timely technical assistance to oper-
23 ators of agency information systems regarding secu-
24 rity incidents, including guidance on detecting and
25 handling information security incidents;

1 “(2) compile and analyze information about in-
2 cidents that threaten information security;

3 “(3) inform operators of agency information
4 systems about current and potential information se-
5 curity threats, and vulnerabilities;

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

11 “(5) consult with the National Institute of
12 Standards and Technology, agencies or offices oper-
13 ating or exercising control of national security sys-
14 tems (including the National Security Agency), and
15 such other agencies or offices in accordance with law
16 and as directed by the President regarding informa-
17 tion security incidents and related matters.

18 “(b) NATIONAL SECURITY SYSTEMS.—Each agency
19 operating or exercising control of a national security sys-
20 tem shall share information about information security in-
21 cidents, threats, and vulnerabilities with the Federal infor-
22 mation security incident center to the extent consistent
23 with standards and guidelines for national security sys-
24 tems, issued in accordance with law and as directed by
25 the President.

1 **“§ 3557. National security systems**

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

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

10 “(2) implements information security policies
11 and practices as required by standards and guide-
12 lines for national security systems, issued in accord-
13 ance with law and as directed by the President; and

14 “(3) complies with the requirements of this sub-
15 chapter.

16 **“§ 3558. Effect on existing law**

17 “Nothing in this subchapter, section 11331 of title
18 40, or section 20 of the National Standards and Tech-
19 nology Act (15 U.S.C. 278g–3) may be construed as af-
20 fecting the authority of the President, the Office of Man-
21 agement and Budget or the Director thereof, the National
22 Institute of Standards and Technology, or the head of any
23 agency, with respect to the authorized use or disclosure
24 of information, including with regard to the protection of
25 personal privacy under section 552a of title 5, the dislo-
26 sure of information under section 552 of title 5, the man-

1 agement and disposition of records under chapters 29, 31,
 2 or 33 of title 44, the management of information resources
 3 under subchapter I of chapter 35 of this title, or the dis-
 4 closure of information to the Congress or the Comptroller
 5 General of the United States.”.

6 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

7 (1) TABLE OF SECTIONS.—The table of sections
 8 for chapter 35 of title 44, United States Code is
 9 amended by striking the matter relating to sub-
 10 chapters 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.”.

11 (2) CYBERSECURITY RESEARCH AND DEVELOP-
 12 MENT ACT.—Section 8(d)(1) of the Cybersecurity
 13 Research and Development Act (15 U.S.C. 7406) is
 14 amended by striking “section 3534” and inserting
 15 “section 3554”.

16 (3) HOMELAND SECURITY ACT OF 2002.—Sec-
 17 tion 1001(c)(1)(A) of the Homeland Security Act of
 18 2002 (6 U.S.C. 511) by striking “section 3532(3)”
 19 and inserting “section 3552(b)(5)”.

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

1 stitute of Standards and Technology Act (15 U.S.C.
2 278g-3) is amended—

3 (A) in subsection (a)(2), by striking “sec-
4 tion 3532(b)(2)” and inserting “section
5 3552(b)(5)”; and

6 (B) in subsection (e)—

7 (i) in paragraph (2), by striking “sec-
8 tion 3532(1)” and inserting “section
9 3552(b)(2)”; and

10 (ii) in paragraph (5), by striking “sec-
11 tion 3532(b)(2)” and inserting “section
12 3552(b)(5)”.

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

15 (A) in section 2222(j)(5), by striking “sec-
16 tion 3542(b)(2)” and inserting “section
17 3552(b)(5)”; and

18 (B) in section 2223(c)(3), by striking “sec-
19 tion 3542(b)(2)” and inserting “section
20 3552(b)(5)”; and

21 (C) in section 2315, by striking “section
22 3542(b)(2)” and inserting “section
23 3552(b)(5)”.

24 (c) OTHER PROVISIONS.—

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

6 (2) ISPAB.—Section 21(b) of the National In-
 7 stitute of Standards and Technology Act (15 U.S.C.
 8 278g-4(b)) is amended—

9 (A) in paragraph (2), by inserting “, the
 10 Secretary of Homeland Security,” after “the
 11 Institute”; and

12 (B) in paragraph (3), by inserting “the
 13 Secretary of Homeland Security,” after “the
 14 Secretary of Commerce,”.

15 **SEC. 3. FEDERAL DATA BREACH RESPONSE GUIDELINES.**

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

19 **“§ 3559. Privacy breach requirements**

20 “(a) POLICIES AND PROCEDURES.—The Director, in
 21 consultation with the Secretary, shall establish and over-
 22 see policies and procedures for agencies to follow in the
 23 event of a breach of information security involving the dis-
 24 closure of personally identifiable information, including re-
 25 quirements for—

1 “(1) timely notice to affected individuals based
2 on a determination of the level of risk and consistent
3 with law enforcement and national security consider-
4 ations;

5 “(2) timely reporting to the Federal informa-
6 tion security incident center established under sec-
7 tion 3556 or other Federal cybersecurity center, as
8 designated by the Director;

9 “(3) timely notice to committees of Congress
10 with jurisdiction over cybersecurity; and

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

15 “(b) CONSIDERATIONS.—In carrying out subsection
16 (a), the Director shall consider recommendations made by
17 the Government Accountability Office, including rec-
18 ommendations in the December 2013 Government Ac-
19 countability Office report entitled ‘Information Security:
20 Agency Responses to Breaches of Personally Identifiable
21 Information Need to Be More Consistent’ (GAO–14–34).

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

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

3 “(d) TIMELINESS.—

4 “(1) IN GENERAL.—Except as provided in para-
5 graph (2), the policies and procedures established
6 under subsection (a) shall require that the notice to
7 affected individuals required under subsection (a)(1)
8 be made without unreasonable delay and with con-
9 sideration of the likely risk of harm and the level of
10 impact, but not later than 60 days after the date on
11 which the head of an agency discovers the breach of
12 information security involving the disclosure of per-
13 sonally identifiable information.

14 “(2) DELAY.—The Attorney General, the head
15 of an element of the intelligence community (as such
16 term is defined under section 3(4) of the National
17 Security Act of 1947 (50 U.S.C. 3003(4)), or the
18 Secretary may delay the notice to affected individ-
19 uals under subsection (a)(1) for not more than 180
20 days, if the notice would disrupt a law enforcement
21 investigation, endanger national security, or hamper
22 security remediation actions from the breach of in-
23 formation security involving the disclosure of person-
24 ally identifiable information.”.

1 (b) TECHNICAL AND CONFORMING AMENDMENT.—
2 The table of sections for subchapter II for chapter 35 of
3 title 44, United States Code, as added by this Act, is
4 amended by inserting after the item relating to section
5 3558 the following:

“3559. Privacy breach requirements.”.

Calendar No. 564

113TH CONGRESS
2^D 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