

113TH CONGRESS
2^D SESSION

S. 2521

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

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

4 **SEC. 2. FISMA REFORM.**

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

8 “SUBCHAPTER II—INFORMATION SECURITY

9 “§ 3551. Purposes

10 “The purposes of this subchapter are to—

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

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

22 “(3) provide for development and maintenance
23 of minimum controls required to protect Federal in-
24 formation and information systems;

25 “(4) provide a mechanism for improved over-
26 sight of Federal agency information security pro-

1 grams, including through automated security tools to
2 continuously diagnose and improve security;

3 “(5) acknowledge that commercially developed
4 information security products offer advanced, dy-
5 namic, robust, and effective information security so-
6 lutions, reflecting market solutions for the protection
7 of critical information infrastructures important to
8 the national defense and economic security of the
9 nation that are designed, built, and operated by the
10 private sector; and

11 “(6) recognize that the selection of specific
12 technical hardware and software information secu-
13 rity solutions should be left to individual agencies
14 from among commercially developed products.

15 **“§ 3552. Definitions**

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

19 “(b) ADDITIONAL DEFINITIONS.—As used in this
20 subchapter:

21 “(1) The term ‘binding operational directive’
22 means a compulsory direction to an agency that—

23 “(A) is for purposes of safeguarding Fed-
24 eral information and information systems from

1 a known or reasonably suspected information
2 security threat, vulnerability, or risk;

3 “(B) shall be in accordance with policies,
4 principles, standards, and guidelines issued by
5 the Director; and

6 “(C) may be revised or repealed by the Di-
7 rector if the direction issued on behalf of the
8 Director is not in accordance with policies and
9 principles developed by the Director.

10 “(2) The term ‘incident’ means an occurrence
11 that—

12 “(A) actually or imminently jeopardizes,
13 without lawful authority, the integrity, con-
14 fidentiality, or availability of information or an
15 information system; or

16 “(B) constitutes a violation or imminent
17 threat of violation of law, security policies, secu-
18 rity procedures, or acceptable use policies.

19 “(3) The term ‘information security’ means
20 protecting information and information systems
21 from unauthorized access, use, disclosure, disrup-
22 tion, modification, or destruction in order to pro-
23 vide—

24 “(A) integrity, which means guarding
25 against improper information modification or

1 destruction, and includes ensuring information
2 nonrepudiation and authenticity;

3 “(B) confidentiality, which means pre-
4 serving authorized restrictions on access and
5 disclosure, including means for protecting per-
6 sonal privacy and proprietary information; and

7 “(C) availability, which means ensuring
8 timely and reliable access to and use of infor-
9 mation.

10 “(4) The term ‘information technology’ has the
11 meaning given that term in section 11101 of title
12 40.

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

16 “(6)(A) The term ‘national security system’
17 means any information system (including any tele-
18 communications system) used or operated by an
19 agency or by a contractor of an agency, or other or-
20 ganization on behalf of an agency—

21 “(i) the function, operation, or use of
22 which—

23 “(I) involves intelligence activities;

24 “(II) involves cryptologic activities re-
25 lated to national security;

1 “(III) involves command and control
2 of military forces;

3 “(IV) involves equipment that is an
4 integral part of a weapon or weapons sys-
5 tem; or

6 “(V) subject to subparagraph (B), is
7 critical to the direct fulfillment of military
8 or intelligence missions; or

9 “(ii) is protected at all times by procedures
10 established for information that have been spe-
11 cifically authorized under criteria established by
12 an Executive order or an Act of Congress to be
13 kept classified in the interest of national de-
14 fense or foreign policy.

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

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

21 **“§ 3553. Authority and functions of the Director and**
22 **the Secretary**

23 “(a) DIRECTOR.—The Director shall oversee agency
24 information security policies and practices, including—

1 “(1) developing and overseeing the implementa-
2 tion of policies, principles, standards, and guidelines
3 on information security, including through ensuring
4 timely agency adoption of and compliance with
5 standards promulgated under section 11331 of title
6 40;

7 “(2) requiring agencies, consistent with the
8 standards promulgated under such section 11331
9 and the requirements of this subchapter, to identify
10 and provide information security protections com-
11 mensurate with the risk and magnitude of the harm
12 resulting from the unauthorized access, use, disclo-
13 sure, disruption, modification, or destruction of—

14 “(A) information collected or maintained
15 by or on behalf of an agency; or

16 “(B) information systems used or operated
17 by an agency or by a contractor of an agency
18 or other organization on behalf of an agency;

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

21 “(4) coordinating the development of standards
22 and guidelines under section 20 of the National In-
23 stitute of Standards and Technology Act (15 U.S.C.
24 278g-3) with agencies and offices operating or exer-
25 cising control of national security systems (including

1 the National Security Agency) to assure, to the max-
2 imum extent feasible, that such standards and
3 guidelines are complementary with standards and
4 guidelines developed for national security systems;

5 “(5) overseeing agency compliance with the re-
6 quirements of this subchapter, including through
7 any authorized action under section 11303 of title
8 40, to enforce accountability for compliance with
9 such requirements; and

10 “(6) coordinating information security policies
11 and procedures with related information resources
12 management policies and procedures.

13 “(b) SECRETARY.—The Secretary, in consultation
14 with the Director, shall administer the implementation of
15 agency information security policies and practices for in-
16 formation systems, except for national security systems
17 and information systems described in paragraph (2) or (3)
18 of subsection (e), including—

19 “(1) assisting the Director in carrying out the
20 authorities and functions under paragraphs (1), (2),
21 (3), (5), and (6) of subsection (a);

22 “(2) developing and overseeing the implementa-
23 tion of binding operational directives to agencies to
24 implement the policies, principles, standards, and
25 guidelines developed by the Director under sub-

1 section (a)(1) and the requirements of this sub-
2 chapter, which may be revised or repealed by the Di-
3 rector if the operational directives issued on behalf
4 of the Director are not in accordance with policies,
5 principles, standards, and guidelines developed by
6 the Director, including—

7 “(A) requirements for reporting security
8 incidents to the Federal information security in-
9 cident center established under section 3556;

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

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

15 “(D) other operational requirements as the
16 Director or Secretary, in consultation with the
17 Director, may determine necessary;

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

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

23 “(5) coordinating Government-wide efforts on
24 information security policies and practices, including
25 consultation with the Chief Information Officers

1 Council established under section 3603 and the Di-
2 rector of the National Institute of Standards and
3 Technology;

4 “(6) providing operational and technical assist-
5 ance to agencies in implementing policies, principles,
6 standards, and guidelines on information security,
7 including implementation of standards promulgated
8 under section 11331 of title 40, including by—

9 “(A) operating the Federal information se-
10 curity incident center established under section
11 3556;

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

16 “(C) compiling and analyzing data on
17 agency information security; and

18 “(D) developing and conducting targeted
19 operational evaluations, including threat and
20 vulnerability assessments, on the information
21 systems; and

22 “(7) other actions as the Director or the Sec-
23 retary, in consultation with the Director, may deter-
24 mine necessary to carry out this subsection.

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

6 “(1) a summary of the incidents described in
7 the annual reports required to be submitted under
8 section 3554(c)(1), including a summary of the in-
9 formation required under section 3554(c)(1)(A)(iii);

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

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

14 “(4) an assessment of agency compliance with
15 standards promulgated under section 11331 of title
16 40; and

17 “(5) an assessment of agency compliance with
18 data breach notification policies and procedures
19 issued by the Director.

20 “(d) NATIONAL SECURITY SYSTEMS.—Except for the
21 authorities and functions described in subsection (a)(5)
22 and subsection (c), the authorities and functions of the
23 Director and the Secretary under this section shall not
24 apply to national security systems.

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

8 “(2) The systems described in this paragraph are sys-
9 tems that are operated by the Department of Defense, a
10 contractor of the Department of Defense, or another enti-
11 ty on behalf of the Department of Defense that processes
12 any information the unauthorized access, use, disclosure,
13 disruption, modification, or destruction of which would
14 have a debilitating impact on the mission of the Depart-
15 ment of Defense.

16 “(3) The systems described in this paragraph are sys-
17 tems that are operated by an element of the intelligence
18 community, a contractor of an element of the intelligence
19 community, or another entity on behalf of an element of
20 the intelligence community that processes any information
21 the unauthorized access, use, disclosure, disruption, modi-
22 fication, or destruction of which would have a debilitating
23 impact on the mission of an element of the intelligence
24 community.

25 “(f) CONSIDERATION.—

1 “(1) IN GENERAL.—In carrying out the respon-
2 sibilities under subsection (b), the Secretary shall
3 consider any applicable standards or guidelines de-
4 veloped by the National Institute of Standards and
5 Technology and issued by the Secretary of Com-
6 merce under section 11331 of title 40.

7 “(2) DIRECTIVES.—The Secretary shall—

8 “(A) consult with the Director of the Na-
9 tional Institute of Standards and Technology
10 regarding any binding operational directive that
11 implements standards and guidelines developed
12 by the National Institute of Standards and
13 Technology; and

14 “(B) ensure that binding operational direc-
15 tives issued under subsection (b)(2) do not con-
16 flict with the standards and guidelines issued
17 under section 11331 of title 40.

18 “(3) RULE OF CONSTRUCTION.—Nothing in
19 this subchapter shall be construed as authorizing the
20 Secretary to direct the Secretary of Commerce in the
21 development and promulgation of standards and
22 guidelines under section 11331 of title 40.

23 “(g) EXERCISE OF AUTHORITY.—To ensure fiscal
24 and policy consistency, the Secretary shall exercise the au-

1 thority under this section subject to direction by the Presi-
2 dent, in coordination with the Director.

3 **“§ 3554. Federal agency responsibilities**

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

5 “(1) be responsible for—

6 “(A) providing information security protec-
7 tions commensurate with the risk and mag-
8 nitude of the harm resulting from unauthorized
9 access, use, disclosure, disruption, modification,
10 or destruction of—

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

13 “(ii) information systems used or op-
14 erated by an agency or by a contractor of
15 an agency or other organization on behalf
16 of an agency;

17 “(B) complying with the requirements of
18 this subchapter and related policies, procedures,
19 standards, and guidelines, including—

20 “(i) information security standards
21 promulgated under section 11331 of title
22 40;

23 “(ii) operational directives developed
24 by the Secretary under section 3553(b);

1 “(iii) policies and procedures issued
2 by the Director; and

3 “(iv) information security standards
4 and guidelines for national security sys-
5 tems issued in accordance with law and as
6 directed by the President; and

7 “(C) ensuring that information security
8 management processes are integrated with
9 agency strategic, operational, and budgetary
10 planning processes;

11 “(2) ensure that senior agency officials provide
12 information security for the information and infor-
13 mation systems that support the operations and as-
14 sets under their control, including through—

15 “(A) assessing the risk and magnitude of
16 the harm that could result from the unauthor-
17 ized access, use, disclosure, disruption, modi-
18 fication, or destruction of such information or
19 information systems;

20 “(B) determining the levels of information
21 security appropriate to protect such information
22 and information systems in accordance with
23 standards promulgated under section 11331 of
24 title 40, for information security classifications
25 and related requirements;

1 “(C) implementing policies and procedures
2 to cost-effectively reduce risks to an acceptable
3 level; and

4 “(D) periodically testing and evaluating in-
5 formation security controls and techniques to
6 ensure that they are effectively implemented;

7 “(3) delegate to the agency Chief Information
8 Officer established under section 3506 (or com-
9 parable official in an agency not covered by such
10 section) the authority to ensure compliance with the
11 requirements imposed on the agency under this sub-
12 chapter, including—

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

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

17 “(ii) possess professional qualifica-
18 tions, including training and experience,
19 required to administer the functions de-
20 scribed under this section;

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

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

1 “(B) developing and maintaining an agen-
2 cywide information security program as re-
3 quired by subsection (b);

4 “(C) developing and maintaining informa-
5 tion security policies, procedures, and control
6 techniques to address all applicable require-
7 ments, including those issued under section
8 3553 of this title and section 11331 of title 40;

9 “(D) training and overseeing personnel
10 with significant responsibilities for information
11 security with respect to such responsibilities;
12 and

13 “(E) assisting senior agency officials con-
14 cerning their responsibilities under paragraph
15 (2);

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

20 “(5) ensure that the agency Chief Information
21 Officer, in coordination with other senior agency of-
22 ficials, reports annually to the agency head on the
23 effectiveness of the agency information security pro-
24 gram, including progress of remedial actions;

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

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

9 “(b) AGENCY PROGRAM.—Each agency shall develop,
10 document, and implement an agency-wide information se-
11 curity program to provide information security for the in-
12 formation and information systems that support the oper-
13 ations and assets of the agency, including those provided
14 or managed by another agency, contractor, or other
15 source, that includes—

16 “(1) periodic assessments of the risk and mag-
17 nitude of the harm that could result from the unau-
18 thorized access, use, disclosure, disruption, modifica-
19 tion, or destruction of information and information
20 systems that support the operations and assets of
21 the agency, which may include using automated
22 tools consistent with standards and guidelines pro-
23 mulgated under section 11331 of title 40;

24 “(2) policies and procedures that—

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

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

5 “(C) ensure that information security is
6 addressed throughout the life cycle of each
7 agency information system; and

8 “(D) ensure compliance with—

9 “(i) the requirements of this sub-
10 chapter;

11 “(ii) policies and procedures as may
12 be prescribed by the Director, and infor-
13 mation security standards promulgated
14 under section 11331 of title 40;

15 “(iii) minimally acceptable system
16 configuration requirements, as determined
17 by the agency; and

18 “(iv) any other applicable require-
19 ments, including standards and guidelines
20 for national security systems issued in ac-
21 cordance with law and as directed by the
22 President;

23 “(3) subordinate plans for providing adequate
24 information security for networks, facilities, and sys-

1 tems or groups of information systems, as appro-
2 priate;

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

7 “(A) information security risks associated
8 with their activities; and

9 “(B) their responsibilities in complying
10 with agency policies and procedures designed to
11 reduce these risks;

12 “(5) periodic testing and evaluation of the ef-
13 fectiveness of information security policies, proce-
14 dures, and practices, to be performed with a fre-
15 quency depending on risk, but no less than annually,
16 of which such testing—

17 “(A) shall include testing of management,
18 operational, and technical controls of every in-
19 formation system identified in the inventory re-
20 quired under section 3505(e);

21 “(B) may include testing relied on in an
22 evaluation under section 3555; and

23 “(C) shall include using automated tools,
24 consistent with standards and guidelines pro-
25 mulgated under section 11331 of title 40;

1 “(6) a process for planning, implementing, eval-
2 uating, and documenting remedial action to address
3 any deficiencies in the information security policies,
4 procedures, and practices of the agency;

5 “(7) procedures for detecting, reporting, and re-
6 sponding to security incidents, which—

7 “(A) shall be consistent with the standards
8 and guidelines described in section 3556(b);

9 “(B) may include using automated tools;
10 and

11 “(C) shall include—

12 “(i) mitigating risks associated with
13 such incidents before substantial damage is
14 done;

15 “(ii) notifying and consulting with the
16 Federal information security incident cen-
17 ter established in section 3556; and

18 “(iii) notifying and consulting with, as
19 appropriate—

20 “(I) law enforcement agencies
21 and relevant Offices of Inspector Gen-
22 eral and Offices of General Counsel;

23 “(II) an office designated by the
24 President for any incident involving a
25 national security system;

1 “(III) for a major incident, the
2 committees of Congress described in
3 subsection (c)(1)—

4 “(aa) not later than 7 days
5 after the date on which there is
6 a reasonable basis to conclude
7 that the major incident has oc-
8 curred; and

9 “(bb) after the initial notifi-
10 cation under item (aa), within a
11 reasonable period of time after
12 additional information relating to
13 the incident is discovered, includ-
14 ing the summary required under
15 subsection (c)(1)(A)(i); and

16 “(IV) any other agency or office,
17 in accordance with law or as directed
18 by the President; and

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

22 “(c) AGENCY REPORTING.—

23 “(1) ANNUAL REPORT.—

24 “(A) IN GENERAL.—Each agency shall
25 submit to the Director, the Secretary, the Com-

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

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

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

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

23 “(III) the status of compliance of
24 the affected information systems with

1 applicable security requirements at
2 the time of the incident; and

3 “(IV) the detection, response,
4 and remediation actions;

5 “(ii) the total number of information
6 security incidents, including a description
7 of incidents resulting in significant com-
8 promise of information security, system
9 impact levels, types of incident, and loca-
10 tions of affected systems;

11 “(iii) a description of each major in-
12 formation security incident that involved a
13 breach of personally identifiable informa-
14 tion, as defined by the Director, includ-
15 ing—

16 “(I) the number of individuals
17 whose information was affected by the
18 major information security incident;
19 and

20 “(II) a description of the infor-
21 mation that was breached or exposed;
22 and

23 “(iv) any other information as the Di-
24 rector or the Secretary, in consultation
25 with the Director, may require.

1 “(B) UNCLASSIFIED REPORT.—

2 “(i) IN GENERAL.—Each report sub-
3 mitted under subparagraph (A) shall be in
4 unclassified form, but may include a classi-
5 fied annex.

6 “(ii) ACCESS TO INFORMATION.—The
7 head of an agency shall ensure that, to the
8 greatest extent practicable, information is
9 included in the unclassified version of the
10 reports submitted by the agency under
11 subparagraph (A).

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

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

21 “(A) the time periods; and

22 “(B) the resources, including budget, staffing,
23 and training,

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

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

4 “(e) PUBLIC NOTICE AND COMMENT.—Each agency
5 shall provide the public with timely notice and opportuni-
6 ties for comment on proposed information security policies
7 and procedures to the extent that such policies and proce-
8 dures affect communication with the public.

9 **“§ 3555. Annual independent evaluation**

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

14 “(2) Each evaluation under this section shall in-
15 clude—

16 “(A) testing of the effectiveness of information
17 security policies, procedures, and practices of a rep-
18 resentative subset of the agency’s information sys-
19 tems;

20 “(B) an assessment of the effectiveness of the
21 information security policies, procedures, and prac-
22 tices of the agency; and

23 “(C) separate presentations, as appropriate, re-
24 garding information security relating to national se-
25 curity systems.

1 “(b) INDEPENDENT AUDITOR.—Subject to sub-
2 section (c)—

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

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

13 “(c) NATIONAL SECURITY SYSTEMS.—For each
14 agency operating or exercising control of a national secu-
15 rity system, that portion of the evaluation required by this
16 section directly relating to a national security system shall
17 be performed—

18 “(1) only by an entity designated by the agency
19 head; and

20 “(2) in such a manner as to ensure appropriate
21 protection for information associated with any infor-
22 mation security vulnerability in such system com-
23 mensurate with the risk and in accordance with all
24 applicable laws.

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

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

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

14 “(f) PROTECTION OF INFORMATION.—Agencies and
15 evaluators shall take appropriate steps to ensure the pro-
16 tection of information which, if disclosed, may adversely
17 affect information security. Such protections shall be com-
18 mensurate with the risk and comply with all applicable
19 laws and regulations.

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

24 “(2) The Director’s report to Congress under this
25 subsection shall summarize information regarding infor-

1 mation security relating to national security systems in
2 such a manner as to ensure appropriate protection for in-
3 formation associated with any information security vulner-
4 ability in such system commensurate with the risk and in
5 accordance with all applicable laws.

6 “(3) Evaluations and any other descriptions of infor-
7 mation systems under the authority and control of the Di-
8 rector of National Intelligence or of National Foreign In-
9 telligence Programs systems under the authority and con-
10 trol of the Secretary of Defense shall be made available
11 to Congress only through the appropriate oversight com-
12 mittees of Congress, in accordance with applicable laws.

13 “(h) COMPTROLLER GENERAL.—The Comptroller
14 General shall periodically evaluate and report to Congress
15 on—

16 “(1) the adequacy and effectiveness of agency
17 information security policies and practices; and

18 “(2) implementation of the requirements of this
19 subchapter.

20 “(i) ASSESSMENT TECHNICAL ASSISTANCE.—The
21 Comptroller General may provide technical assistance to
22 an Inspector General or the head of an agency, as applica-
23 ble, to assist the Inspector General or head of an agency
24 in carrying out the duties under this section, including by
25 testing information security controls and procedures.

1 “(j) GUIDANCE.—The Director, in consultation with
2 the Secretary, the Chief Information Officers Council es-
3 tablished under section 3603, the Council of the Inspec-
4 tors General on Integrity and Efficiency, and other inter-
5 ested parties as appropriate, shall ensure the development
6 of guidance for evaluating the effectiveness of an informa-
7 tion security program and practices.

8 **“§ 3556. Federal information security incident center**

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

12 “(1) provide timely technical assistance to oper-
13 ators of agency information systems regarding secu-
14 rity incidents, including guidance on detecting and
15 handling information security incidents;

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

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

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

1 “(5) consult with the National Institute of
2 Standards and Technology, agencies or offices oper-
3 ating or exercising control of national security sys-
4 tems (including the National Security Agency), and
5 such other agencies or offices in accordance with law
6 and as directed by the President regarding informa-
7 tion security incidents and related matters.

8 “(b) NATIONAL SECURITY SYSTEMS.—Each agency
9 operating or exercising control of a national security sys-
10 tem shall share information about information security in-
11 cidents, threats, and vulnerabilities with the Federal infor-
12 mation security incident center to the extent consistent
13 with standards and guidelines for national security sys-
14 tems, issued in accordance with law and as directed by
15 the President.

16 **“§ 3557. National security systems**

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

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

1 “(2) implements information security policies
2 and practices as required by standards and guide-
3 lines for national security systems, issued in accord-
4 ance with law and as directed by the President; and
5 “(3) complies with the requirements of this sub-
6 chapter.

7 **“§ 3558. Effect on existing law**

8 “Nothing in this subchapter, section 11331 of title
9 40, or section 20 of the National Standards and Tech-
10 nology Act (15 U.S.C. 278g–3) may be construed as af-
11 fecting the authority of the President, the Office of Man-
12 agement and Budget or the Director thereof, the National
13 Institute of Standards and Technology, or the head of any
14 agency, with respect to the authorized use or disclosure
15 of information, including with regard to the protection of
16 personal privacy under section 552a of title 5, the disclo-
17 sure of information under section 552 of title 5, the man-
18 agement and disposition of records under chapters 29, 31,
19 or 33 of title 44, the management of information resources
20 under subchapter I of chapter 35 of this title, or the dis-
21 closure of information to the Congress or the Comptroller
22 General of the United States.”.

23 (b) MAJOR INCIDENT.—The Director of the Office of
24 Management and Budget shall—

1 (1) develop guidance on what constitutes a
2 major incident for purposes of section 3554(b) of
3 title 44, United States Code, as added by subsection
4 (a); and

5 (2) provide to Congress periodic briefings on
6 the status of the developing of the guidance until the
7 date on which the guidance is issued.

8 (c) CONTINUOUS DIAGNOSTICS.—During the 2 year
9 period beginning on the date of enactment of this Act, the
10 Director of the Office of Management and Budget, with
11 the assistance of the Secretary of Homeland Security,
12 shall include in each report submitted under section
13 3553(c) of title 44, United States Code, as added by sub-
14 section (a), an assessment of the adoption by agencies of
15 continuous diagnostics technologies, including through the
16 Continuous Diagnostics and Mitigation program, and
17 other advanced security tools to provide information secu-
18 rity, including challenges to the adoption of such tech-
19 nologies or security tools.

20 (d) BREACHES.—

21 (1) REQUIREMENTS.—The Director of the Of-
22 fice of Management and Budget shall ensure that
23 data breach notification policies and guidelines are
24 updated periodically and require—

1 (A) except as provided in paragraph (4),
2 notice by the affected agency to each committee
3 of Congress described in section 3554(e)(1) of
4 title 44, United States Code, as added by sub-
5 section (a), the Committee on the Judiciary of
6 the Senate, and the Committee on the Judiciary
7 of the House of Representatives, which shall—

8 (i) be provided expeditiously and not
9 later than 30 days after the date on which
10 the agency discovered the unauthorized ac-
11 quisition or access; and

12 (ii) include—

13 (I) information about the breach,
14 including a summary of any informa-
15 tion that the agency knows on the
16 date on which notification is provided
17 about how the breach occurred;

18 (II) an estimate of the number of
19 individuals affected by the breach,
20 based on information that the agency
21 knows on the date on which notifica-
22 tion is provided, including an assess-
23 ment of the risk of harm to affected
24 individuals;

1 (III) a description of any cir-
2 cumstances necessitating a delay in
3 providing notice to affected individ-
4 uals; and

5 (IV) an estimate of whether and
6 when the agency will provide notice to
7 affected individuals; and

8 (B) notice by the affected agency to af-
9 fected individuals, pursuant to data breach noti-
10 fication policies and guidelines, which shall be
11 provided as expeditiously as practicable and
12 without unreasonable delay after the agency
13 discovers the unauthorized acquisition or ac-
14 cess.

15 (2) NATIONAL SECURITY; LAW ENFORCEMENT;
16 REMEDIATION.—The Attorney General, the head of
17 an element of the intelligence community (as such
18 term is defined under section 3(4) of the National
19 Security Act of 1947 (50 U.S.C. 3003(4)), or the
20 Secretary of Homeland Security may delay the no-
21 tice to affected individuals under paragraph (1)(B)
22 if the notice would disrupt a law enforcement inves-
23 tigation, endanger national security, or hamper secu-
24 rity remediation actions.

25 (3) REPORTS.—

1 (A) DIRECTOR OF OMB.—During the first
2 2 years beginning after the date of enactment
3 of this Act, the Director of the Office of Man-
4 agement and Budget shall, on an annual
5 basis—

6 (i) assess agency implementation of
7 data breach notification policies and guide-
8 lines in aggregate; and

9 (ii) include the assessment described
10 in clause (i) in the report required under
11 section 3553(e) of title 44, United States
12 Code.

13 (B) SECRETARY OF HOMELAND SECUR-
14 ITY.—During the first 2 years beginning after
15 the date of enactment of this Act, the Secretary
16 of Homeland Security shall include an assess-
17 ment of the status of agency implementation of
18 data breach notification policies and guidelines
19 in the requirements under section
20 3553(b)(2)(B) of title 44, United States Code.

21 (4) EXCEPTION.—Any element of the intel-
22 ligence community (as such term is defined under
23 section 3(4) of the National Security Act of 1947
24 (50 U.S.C. 3003(4)) that is required to provide no-

1 tice under paragraph (1)(A) shall only provide such
2 notice to appropriate committees of Congress.

3 (5) RULE OF CONSTRUCTION.—Nothing in
4 paragraph (1) shall be construed to alter any au-
5 thority of a Federal agency or department.

6 (e) 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.—The
17 Homeland Security Act of 2002 (6 U.S.C. 101 et
18 seq.) is amended—

19 (A) in section 223 (6 U.S.C. 143)

1 (i) in the section heading, by inserting
2 “**FEDERAL AND**” before “**NON-FED-**
3 **ERAL**”;

4 (ii) in the matter preceding paragraph
5 (1), by striking “the Under Secretary for
6 Intelligence and Analysis, in cooperation
7 with the Assistant Secretary for Infra-
8 structure Protection” and inserting “the
9 Under Secretary appointed under section
10 103(a)(1)(H)”;

11 (iii) in paragraph (2), by striking the
12 period at the end and inserting “; and”;
13 and

14 (iv) by adding at the end the fol-
15 lowing:

16 “(3) fulfill the responsibilities of the Secretary
17 to protect Federal information systems under sub-
18 chapter II of chapter 35 of title 44, United States
19 Code.”;

20 (B) in section 1001(e)(1)(A) (6 U.S.C.
21 511(c)(1)(A)), by striking “section 3532(3)”
22 and inserting “section 3552(b)(5)”;

23 (C) in the table of contents in section 1(b),
24 by striking the item relating to section 223 and
25 inserting the following:

“Sec. 223. Enhancement of Federal and non-Federal cybersecurity.”.

1 (4) NATIONAL INSTITUTE OF STANDARDS AND
2 TECHNOLOGY ACT.—Section 20 of the National In-
3 stitute of Standards and Technology Act (15 U.S.C.
4 278g-3) is amended—

5 (A) in subsection (a)(2), by striking “sec-
6 tion 3532(b)(2)” and inserting “section
7 3552(b)(5)”; and

8 (B) in subsection (e)—

9 (i) in paragraph (2), by striking “sec-
10 tion 3532(1)” and inserting “section
11 3552(b)(2)”; and

12 (ii) in paragraph (5), by striking “sec-
13 tion 3532(b)(2)” and inserting “section
14 3552(b)(5)”.

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

17 (A) in section 2222(j)(5), by striking “sec-
18 tion 3542(b)(2)” and inserting “section
19 3552(b)(5)”; and

20 (B) in section 2223(c)(3), by striking “sec-
21 tion 3542(b)(2)” and inserting “section
22 3552(b)(5)”; and

23 (C) in section 2315, by striking “section
24 3542(b)(2)” and inserting “section
25 3552(b)(5)”.

1 (f) OTHER PROVISIONS.—

2 (1) CIRCULAR A–130.—Not later than 1 year
3 after the date of enactment of this Act, the Director
4 of the Office of Management and Budget shall
5 amend or revise Office of Management and Budget
6 Circular A–130 to eliminate inefficient or wasteful
7 reporting. The Director of the Office of Management
8 and Budget shall provide quarterly briefings to Con-
9 gress on the status of the amendment or revision re-
10 quired under this paragraph.

11 (2) ISPAB.—Section 21(b) of the National In-
12 stitute of Standards and Technology Act (15 U.S.C.
13 278g–4(b)) is amended—

14 (A) in paragraph (2), by inserting “, the
15 Secretary of Homeland Security,” after “the
16 Institute”; and

17 (B) in paragraph (3), by inserting “the
18 Secretary of Homeland Security,” after “the
19 Secretary of Commerce.”

Passed the Senate December 8, 2014.

Attest:

Secretary.

113TH CONGRESS
2^D SESSION

S. 2521

AN ACT

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