

Union Calendar No. 26

113TH CONGRESS
1ST SESSION

H. R. 1163

[Report No. 113-40]

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 14, 2013

Mr. ISSA (for himself, Mr. CUMMINGS, Mr. MICA, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

APRIL 16, 2013

Additional sponsors: Mr. CHAFFETZ and Mr. TIERNEY

APRIL 16, 2013

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

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

A BILL

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

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 Amendments Act of 2013”.

6 **SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-**
7 **ICY.**

8 Chapter 35 of title 44, United States Code, is amend-
9 ed by striking subchapters II and III and inserting the
10 following:

11 “SUBCHAPTER II—INFORMATION SECURITY

12 **“§ 3551. Purposes**

13 “The purposes of this subchapter are to—

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

18 “(2) recognize the highly networked nature of
19 the current Federal computing environment and pro-
20 vide effective Governmentwide management and
21 oversight of the related information security risks,
22 including coordination of information security efforts
23 throughout the civilian, national security, and law
24 enforcement communities assets;

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

4 “(4) provide a mechanism for improved over-
5 sight of Federal agency information security pro-
6 grams and systems through a focus on automated
7 and continuous monitoring of agency information
8 systems and regular threat assessments;

9 “(5) acknowledge that commercially developed
10 information security products offer advanced, dy-
11 namic, robust, and effective information security so-
12 lutions, reflecting market solutions for the protection
13 of critical information systems important to the na-
14 tional defense and economic security of the Nation
15 that are designed, built, and operated by the private
16 sector; and

17 “(6) recognize that the selection of specific
18 technical hardware and software information secu-
19 rity solutions should be left to individual agencies
20 from among commercially developed products.

21 **“§ 3552. Definitions**

22 “(a) SECTION 3502 DEFINITIONS.—Except as pro-
23 vided under subsection (b), the definitions under section
24 3502 shall apply to this subchapter.

25 “(b) ADDITIONAL DEFINITIONS.—In this subchapter:

1 “(1) ADEQUATE SECURITY.—The term ‘ade-
2 quate security’ means security commensurate with
3 the risk and magnitude of the harm resulting from
4 the unauthorized access to or loss, misuse, destruc-
5 tion, or modification of information.

6 “(2) AUTOMATED AND CONTINUOUS MONI-
7 TORING.—The term ‘automated and continuous
8 monitoring’ means monitoring, with minimal human
9 involvement, through an uninterrupted, ongoing real
10 time, or near real-time process used to determine if
11 the complete set of planned, required, and deployed
12 security controls within an information system con-
13 tinue to be effective over time with rapidly changing
14 information technology and threat development.

15 “(3) INCIDENT.—The term ‘incident’ means an
16 occurrence that actually or potentially jeopardizes
17 the confidentiality, integrity, or availability of an in-
18 formation system, or the information the system
19 processes, stores, or transmits or that constitutes a
20 violation or imminent threat of violation of security
21 policies, security procedures, or acceptable use poli-
22 cies.

23 “(4) INFORMATION SECURITY.—The term ‘in-
24 formation security’ means protecting information
25 and information systems from unauthorized access,

1 use, disclosure, disruption, modification, or destruc-
2 tion in order to provide—

3 “(A) integrity, which means guarding
4 against improper information modification or
5 destruction, and includes ensuring information
6 nonrepudiation and authenticity;

7 “(B) confidentiality, which means pre-
8 serving authorized restrictions on access and
9 disclosure, including means for protecting per-
10 sonal privacy and proprietary information; and

11 “(C) availability, which means ensuring
12 timely and reliable access to and use of infor-
13 mation.

14 “(5) INFORMATION SYSTEM.—The term ‘infor-
15 mation system’ means a discrete set of information
16 resources organized for the collection, processing,
17 maintenance, use, sharing, dissemination, or disposi-
18 tion of information and includes—

19 “(A) computers and computer networks;

20 “(B) ancillary equipment;

21 “(C) software, firmware, and related proce-
22 dures;

23 “(D) services, including support services;

24 and

25 “(E) related resources.

1 “(6) INFORMATION TECHNOLOGY.—The term
2 ‘information technology’ has the meaning given that
3 term in section 11101 of title 40.

4 “(7) NATIONAL SECURITY SYSTEM.—

5 “(A) DEFINITION.—The term ‘national se-
6 curity system’ means any information system
7 (including any telecommunications system) used
8 or operated by an agency or by a contractor of
9 an agency, or other organization on behalf of an
10 agency—

11 “(i) the function, operation, or use of
12 which—

13 “(I) involves intelligence activi-
14 ties;

15 “(II) involves cryptologic activi-
16 ties related to national security;

17 “(III) involves command and
18 control of military forces;

19 “(IV) involves equipment that is
20 an integral part of a weapon or weap-
21 ons system; or

22 “(V) subject to subparagraph
23 (B), is critical to the direct fulfillment
24 of military or intelligence missions; or

1 “(ii) is protected at all times by proce-
2 dures established for information that have
3 been specifically authorized under criteria
4 established by an Executive order or an
5 Act of Congress to be kept classified in the
6 interest of national defense or foreign pol-
7 icy.

8 “(B) EXCEPTION.—Subparagraph
9 (A)(i)(V) does not include a system that is to
10 be used for routine administrative and business
11 applications (including payroll, finance, logis-
12 tics, and personnel management applications).

13 “(8) THREAT ASSESSMENT.—The term ‘threat
14 assessment’ means the formal description and eval-
15 uation of threat to an information system.

16 **“§ 3553. Authority and functions of the Director**

17 “(a) IN GENERAL.—The Director shall oversee agen-
18 cy information security policies and practices, including—

19 “(1) developing and overseeing the implementa-
20 tion of policies, principles, standards, and guidelines
21 on information security, including through ensuring
22 timely agency adoption of and compliance with
23 standards promulgated under section 11331 of title
24 40;

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

8 “(A) information collected or maintained
9 by or on behalf of an agency; or

10 “(B) information systems used or operated
11 by an agency or by a contractor of an agency
12 or other organization on behalf of an agency;

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

22 “(4) overseeing agency compliance with the re-
23 quirements of this subchapter, including through
24 any authorized action under section 11303 of title

1 40, to enforce accountability for compliance with
2 such requirements;

3 “(5) reviewing at least annually, and approving
4 or disapproving, agency information security pro-
5 grams required under section 3554(b);

6 “(6) coordinating information security policies
7 and procedures with related information resources
8 management policies and procedures;

9 “(7) overseeing the operation of the Federal in-
10 formation security incident center required under
11 section 3555; and

12 “(8) reporting to Congress no later than March
13 1 of each year on agency compliance with the re-
14 quirements of this subchapter, including—

15 “(A) an assessment of the development,
16 promulgation, and adoption of, and compliance
17 with, standards developed under section 20 of
18 the National Institute of Standards and Tech-
19 nology Act (15 U.S.C. 278g–3) and promul-
20 gated under section 11331 of title 40;

21 “(B) significant deficiencies in agency in-
22 formation security practices;

23 “(C) planned remedial action to address
24 such deficiencies; and

1 “(D) a summary of, and the views of the
2 Director on, the report prepared by the Na-
3 tional Institute of Standards and Technology
4 under section 20(d)(10) of the National Insti-
5 tute of Standards and Technology Act (15
6 U.S.C. 278g-3).

7 “(b) NATIONAL SECURITY SYSTEMS.—Except for the
8 authorities described in paragraphs (4) and (8) of sub-
9 section (a), the authorities of the Director under this sec-
10 tion shall not apply to national security systems.

11 “(c) DEPARTMENT OF DEFENSE AND CENTRAL IN-
12 TELLIGENCE AGENCY SYSTEMS.—(1) The authorities of
13 the Director described in paragraphs (1) and (2) of sub-
14 section (a) shall be delegated to the Secretary of Defense
15 in the case of systems described in paragraph (2) and to
16 the Director of Central Intelligence in the case of systems
17 described in paragraph (3).

18 “(2) The systems described in this paragraph are sys-
19 tems that are operated by the Department of Defense, a
20 contractor of the Department of Defense, or another enti-
21 ty on behalf of the Department of Defense that processes
22 any information the unauthorized access, use, disclosure,
23 disruption, modification, or destruction of which would
24 have a debilitating impact on the mission of the Depart-
25 ment of Defense.

1 “(3) The systems described in this paragraph are sys-
2 tems that are operated by the Central Intelligence Agency,
3 a contractor of the Central Intelligence Agency, or another
4 entity on behalf of the Central Intelligence Agency that
5 processes any information the unauthorized access, use,
6 disclosure, disruption, modification, or destruction of
7 which would have a debilitating impact on the mission of
8 the Central Intelligence Agency.

9 **“§ 3554. Agency responsibilities**

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

11 “(1) be responsible for—

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

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

19 “(ii) information systems used or op-
20 erated by an agency or by a contractor of
21 an agency or other organization on behalf
22 of an agency;

23 “(B) complying with the requirements of
24 this subchapter and related policies, procedures,
25 standards, and guidelines, including—

1 “(i) information security standards
2 and guidelines promulgated under section
3 11331 of title 40 and section 20 of the Na-
4 tional Institute of Standards and Tech-
5 nology Act (15 U.S.C. 278g-3);

6 “(ii) information security standards
7 and guidelines for national security sys-
8 tems issued in accordance with law and as
9 directed by the President; and

10 “(iii) ensuring the standards imple-
11 mented for information systems and na-
12 tional security systems of the agency are
13 complementary and uniform, to the extent
14 practicable;

15 “(C) ensuring that information security
16 management processes are integrated with
17 agency strategic and operational planning and
18 budget processes, including policies, procedures,
19 and practices described in subsection (c)(2);

20 “(D) as appropriate, maintaining secure
21 facilities that have the capability of accessing,
22 sending, receiving, and storing classified infor-
23 mation;

24 “(E) maintaining a sufficient number of
25 personnel with security clearances, at the ap-

1 appropriate levels, to access, send, receive and
2 analyze classified information to carry out the
3 responsibilities of this subchapter; and

4 “(F) ensuring that information security
5 performance indicators and measures are in-
6 cluded in the annual performance evaluations of
7 all managers, senior managers, senior executive
8 service personnel, and political appointees;

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

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

18 “(B) determining the levels of information
19 security appropriate to protect such information
20 and information systems in accordance with
21 policies, principles, standards, and guidelines
22 promulgated under section 11331 of title 40
23 and section 20 of the National Institute of
24 Standards and Technology Act (15 U.S.C.

1 278g–3) for information security classifications
2 and related requirements;

3 “(C) implementing policies and procedures
4 to cost effectively reduce risks to an acceptable
5 level;

6 “(D) with a frequency sufficient to support
7 risk-based security decisions, testing and evalu-
8 ating information security controls and tech-
9 niques to ensure that such controls and tech-
10 niques are effectively implemented and oper-
11 ated; and

12 “(E) with a frequency sufficient to support
13 risk-based security decisions, conducting threat
14 assessments by monitoring information systems,
15 identifying potential system vulnerabilities, and
16 reporting security incidents in accordance with
17 paragraph (3)(A)(v);

18 “(3) delegate to the Chief Information Officer
19 or equivalent (or a senior agency official who reports
20 to the Chief Information Officer or equivalent), who
21 is designated as the ‘Chief Information Security Of-
22 ficer’, the authority and primary responsibility to de-
23 velop, implement, and oversee an agencywide infor-
24 mation security program to ensure and enforce com-

1 pliance with the requirements imposed on the agency
2 under this subchapter, including—

3 “(A) overseeing the establishment and
4 maintenance of a security operations capability
5 that through automated and continuous moni-
6 toring, when possible, can—

7 “(i) detect, report, respond to, con-
8 tain, and mitigate incidents that impair in-
9 formation security and agency information
10 systems, in accordance with policy provided
11 by the Director;

12 “(ii) commensurate with the risk to
13 information security, monitor and mitigate
14 the vulnerabilities of every information sys-
15 tem within the agency;

16 “(iii) continually evaluate risks posed
17 to information collected or maintained by
18 or on behalf of the agency and information
19 systems and hold senior agency officials
20 accountable for ensuring information secu-
21 rity;

22 “(iv) collaborate with the Director and
23 appropriate public and private sector secu-
24 rity operations centers to detect, report, re-
25 spond to, contain, and mitigate incidents

1 that impact the security of information
2 and information systems that extend be-
3 yond the control of the agency; and

4 “(v) report any incident described
5 under clauses (i) and (ii) to the Federal in-
6 formation security incident center, to other
7 appropriate security operations centers,
8 and to the Inspector General of the agen-
9 cy, to the extent practicable, within 24
10 hours after discovery of the incident, but
11 no later than 48 hours after such dis-
12 covery;

13 “(B) developing, maintaining, and over-
14 seeing an agencywide information security pro-
15 gram as required by subsection (b);

16 “(C) developing, maintaining, and over-
17 seeing information security policies, procedures,
18 and control techniques to address all applicable
19 requirements, including those issued under sec-
20 tion 11331 of title 40;

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

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

4 “(4) ensure that the agency has a sufficient
5 number of trained and cleared personnel to assist
6 the agency in complying with the requirements of
7 this subchapter, other applicable laws, and related
8 policies, procedures, standards, and guidelines;

9 “(5) ensure that the Chief Information Security
10 Officer, in consultation with other senior agency offi-
11 cials, reports periodically, but not less than annually,
12 to the agency head on—

13 “(A) the effectiveness of the agency infor-
14 mation security program;

15 “(B) information derived from automated
16 and continuous monitoring, when possible, and
17 threat assessments; and

18 “(C) the progress of remedial actions;

19 “(6) ensure that the Chief Information Security
20 Officer possesses the necessary qualifications, includ-
21 ing education, training, experience, and the security
22 clearance required to administer the functions de-
23 scribed under this subchapter; and has information
24 security duties as the primary duty of that official;
25 and

1 “(7) ensure that components of that agency es-
2 tablish and maintain an automated reporting mecha-
3 nism that allows the Chief Information Security Of-
4 ficer with responsibility for the entire agency, and all
5 components thereof, to implement, monitor, and hold
6 senior agency officers accountable for the implemen-
7 tation of appropriate security policies, procedures,
8 and controls of agency components.

9 “(b) AGENCY PROGRAM.—Each agency shall develop,
10 document, and implement an agencywide information se-
11 curity program, approved by the Director and consistent
12 with components across and within agencies, to provide
13 information security for the information and information
14 systems that support the operations and assets of the
15 agency, including those provided or managed by another
16 agency, contractor, or other source, that includes—

17 “(1) automated and continuous monitoring,
18 when possible, of the risk and magnitude of the
19 harm that could result from the disruption or unau-
20 thorized access, use, disclosure, modification, or de-
21 struction of information and information systems
22 that support the operations and assets of the agen-
23 cy;

24 “(2) consistent with guidance developed under
25 section 11331 of title 40, vulnerability assessments

1 and penetration tests commensurate with the risk
2 posed to agency information systems;

3 “(3) policies and procedures that—

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

6 “(B) ensure compliance with—

7 “(i) the requirements of this sub-
8 chapter;

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

13 “(iii) minimally acceptable system
14 configuration requirements, as determined
15 by the Director; and

16 “(iv) any other applicable require-
17 ments, including—

18 “(I) standards and guidelines for
19 national security systems issued in ac-
20 cordance with law and as directed by
21 the President; and

22 “(II) the National Institute of
23 Standards and Technology standards
24 and guidance;

1 “(C) develop, maintain, and oversee infor-
2 mation security policies, procedures, and control
3 techniques to address all applicable require-
4 ments, including those promulgated pursuant
5 section 11331 of title 40; and

6 “(D) ensure the oversight and training of
7 personnel with significant responsibilities for in-
8 formation security with respect to such respon-
9 sibilities;

10 “(4) with a frequency sufficient to support risk-
11 based security decisions, automated and continuous
12 monitoring, when possible, for testing and evaluation
13 of the effectiveness and compliance of information
14 security policies, procedures, and practices, includ-
15 ing—

16 “(A) controls of every information system
17 identified in the inventory required under sec-
18 tion 3505(e); and

19 “(B) controls relied on for an evaluation
20 under this section;

21 “(5) a process for planning, implementing, eval-
22 uating, and documenting remedial action to address
23 any deficiencies in the information security policies,
24 procedures, and practices of the agency;

1 “(6) with a frequency sufficient to support risk-
2 based security decisions, automated and continuous
3 monitoring, when possible, for detecting, reporting,
4 and responding to security incidents, consistent with
5 standards and guidelines issued by the National In-
6 stitute of Standards and Technology, including—

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

9 “(B) notifying and consulting with the
10 Federal information security incident center
11 and other appropriate security operations re-
12 sponse centers; and

13 “(C) notifying and consulting with, as ap-
14 propriate—

15 “(i) law enforcement agencies and rel-
16 evant Offices of Inspectors General; and

17 “(ii) any other agency, office, or enti-
18 ty, in accordance with law or as directed
19 by the President; and

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

23 “(c) AGENCY REPORTING.—Each agency shall—

24 “(1) submit an annual report on the adequacy
25 and effectiveness of information security policies,

1 procedures, and practices, and compliance with the
2 requirements of this subchapter, including compli-
3 ance with each requirement of subsection (b) to—

4 “(A) the Director;

5 “(B) the Committee on Homeland Security
6 and Governmental Affairs of the Senate;

7 “(C) the Committee on Oversight and Gov-
8 ernment Reform of the House of Representa-
9 tives;

10 “(D) other appropriate authorization and
11 appropriations committees of Congress; and

12 “(E) the Comptroller General;

13 “(2) address the adequacy and effectiveness of
14 information security policies, procedures, and prac-
15 tices in plans and reports relating to—

16 “(A) annual agency budgets;

17 “(B) information resources management of
18 this subchapter;

19 “(C) information technology management
20 under this chapter;

21 “(D) program performance under sections
22 1105 and 1115 through 1119 of title 31, and
23 sections 2801 and 2805 of title 39;

24 “(E) financial management under chapter
25 9 of title 31, and the Chief Financial Officers

1 Act of 1990 (31 U.S.C. 501 note; Public Law
2 101–576);

3 “(F) financial management systems under
4 the Federal Financial Management Improve-
5 ment Act of 1996 (31 U.S.C. 3512 note); and

6 “(G) internal accounting and administra-
7 tive controls under section 3512 of title 31; and

8 “(3) report any significant deficiency in a pol-
9 icy, procedure, or practice identified under para-
10 graph (1) or (2)—

11 “(A) as a material weakness in reporting
12 under section 3512 of title 31; and

13 “(B) if relating to financial management
14 systems, as an instance of a lack of substantial
15 compliance under the Federal Financial Man-
16 agement Improvement Act of 1996 (31 U.S.C.
17 3512 note).

18 **“§ 3555. Federal information security incident center**

19 “(a) IN GENERAL.—The Director 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; and

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

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

21 “(c) REVIEW AND APPROVAL.—The Director shall
22 review and approve the policies, procedures, and guidance
23 established in this subchapter to ensure that the incident
24 center has the capability to effectively and efficiently de-
25 tect, correlate, respond to, contain, mitigate, and reme-

1 diate incidents that impair the adequate security of the
 2 information systems of more than one agency. To the ex-
 3 tent practicable, the capability shall be continuous and
 4 technically automated.

5 **“§ 3556. National security systems**

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

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

14 “(2) implements information security policies
 15 and practices as required by standards and guide-
 16 lines for national security systems, issued in accord-
 17 ance with law and as directed by the President; and

18 “(3) complies with the requirements of this sub-
 19 chapter.”.

20 **SEC. 3. TECHNICAL AND CONFORMING AMENDMENTS.**

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

“SUBCHAPTER II—INFORMATION SECURITY

“Sec.

“3551. Purposes.

“3552. Definitions.

“3553. Authority and functions of the Director.

“3554. Agency responsibilities.

“3555. Federal information security incident center.

“3556. National security systems.”.

1 (b) OTHER REFERENCES.—

2 (1) Section 1001(c)(1)(A) of the Homeland Se-
 3 curity Act of 2002 (6 U.S.C. 511(c)(1)(A)) is
 4 amended by striking “section 3532(3)” and insert-
 5 ing “section 3552(b)”.

6 (2) Section 2222(j)(5) of title 10, United States
 7 Code, is amended by striking “section 3542(b)(2)”
 8 and inserting “section 3552(b)”.

9 (3) Section 2223(c)(3) of title 10, United
 10 States Code, is amended, by striking “section
 11 3542(b)(2)” and inserting “section 3552(b)”.

12 (4) Section 2315 of title 10, United States
 13 Code, is amended by striking “section 3542(b)(2)”
 14 and inserting “section 3552(b)”.

15 (5) Section 20 of the National Institute of
 16 Standards and Technology Act (15 U.S.C. 278g–3)
 17 is amended—

18 (A) in ~~subsections (a)(2) and (e)(5)~~ *sub-*
 19 *section (a)(2)*, by striking “section 3532(b)(2)”
 20 and inserting “section 3552(b)”; and

21 (B) in subsection (e)—

1 (i) in paragraph (2), by striking “sec-
2 tion 3532(1)” and inserting “section
3 3552(b)”;

4 (ii) in paragraph (5), by striking “sec-
5 tion 3532(b)(2)” and inserting “section
6 3552(b)”.

7 (6) Section 8(d)(1) of the Cyber Security Re-
8 search and Development Act (15 U.S.C. 7406(d)(1))
9 is amended by striking “section 3534(b)” and in-
10 serting “section 3554(b)”.

11 **SEC. 4. NO ADDITIONAL FUNDS AUTHORIZED.**

12 No additional funds are authorized to carry out the
13 requirements of section 3554 of title 44, United States
14 Code, as amended by section 2 of this Act. Such require-
15 ments shall be carried out using amounts otherwise au-
16 thorized or appropriated.

17 **SEC. 5. EFFECTIVE DATE.**

18 This Act (including the amendments made by this
19 Act) shall take effect 30 days after the date of the enact-
20 ment of this Act.

Union Calendar No. 26

113TH CONGRESS
1ST Session

H. R. 1163

[Report No. 113-40]

A BILL

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

APRIL 16, 2013

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed