

Union Calendar No. 318

112TH CONGRESS
2^D SESSION

H. R. 4257

[Report No. 112–455]

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 26, 2012

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

APRIL 26, 2012

Additional sponsor: Mr. VAN HOLLEN

APRIL 26, 2012

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

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on March 26, 2012]

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 Se-*
5 *curity Amendments Act of 2012”.*

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

8 *Chapter 35 of title 44, United States Code, is amended*
9 *by striking subchapters II and III and inserting the fol-*
10 *lowing:*

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 *sureing the effectiveness of information security con-*
16 *trols over information resources that support Federal*
17 *operations and assets;*

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

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

4 “(4) provide a mechanism for improved oversight
5 of Federal agency information security programs and
6 systems through a focus on automated and continuous
7 monitoring of agency information systems and reg-
8 ular threat assessments;

9 “(5) acknowledge that commercially developed
10 information security products offer advanced, dy-
11 namic, robust, and effective information security solu-
12 tions, reflecting market solutions for the protection of
13 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 tech-
18 nical hardware and software information security so-
19 lutions should be left to individual agencies from
20 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 ‘adequate
2 *security*’ means security commensurate with the risk
3 and magnitude of the harm resulting from the unau-
4 thorized access to or loss, misuse, destruction, or
5 modification of information.

6 “(2) *AUTOMATED AND CONTINUOUS MONI-*
7 *TORING.*—The term ‘automated and continuous moni-
8 toring’ means monitoring, with minimal human in-
9 volvement, 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 se-
12 curity 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 the
17 confidentiality, integrity, or availability of an infor-
18 mation system, or the information the system proc-
19 esses, stores, or transmits or that constitutes a viola-
20 tion or imminent threat of violation of security poli-
21 cies, security procedures, or acceptable use policies.

22 “(4) *INFORMATION SECURITY.*—The term ‘infor-
23 mation security’ means protecting information and
24 information systems from unauthorized access, use,

1 *disclosure, disruption, modification, or destruction in*
2 *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 *servicing authorized restrictions on access and dis-*
9 *closure, including means for protecting personal*
10 *privacy and proprietary information; and*

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

14 “(5) *INFORMATION SYSTEM.—The term ‘informa-*
15 *tion system’ means a discrete set of information re-*
16 *sources organized for the collection, processing, main-*
17 *tenance, use, sharing, dissemination, or disposition of*
18 *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 ‘in-*
2 *formation 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 con-*
18 *trol 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 (B),*
23 *is critical to the direct fulfillment of*
24 *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 Act
5 of Congress to be kept classified in the inter-
6 est of national defense or foreign policy.

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

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

15 **“§ 3553. Authority and functions of the Director**

16 “(a) IN GENERAL.—The Director shall oversee agency
17 information security policies and practices, including—

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

24 “(2) requiring agencies, consistent with the
25 standards promulgated under such section 11331 and

1 *the requirements of this subchapter, to identify and*
2 *provide information security protections commensu-*
3 *rate with the risk and magnitude of the harm result-*
4 *ing from the unauthorized access, use, disclosure, dis-*
5 *ruption, modification, or destruction of—*

6 “(A) *information collected or maintained by*
7 *or on behalf of an agency; or*

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

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

20 “(4) *overseeing agency compliance with the re-*
21 *quirements of this subchapter, including through any*
22 *authorized action under section 11303 of title 40, to*
23 *enforce accountability for compliance with such re-*
24 *quirements;*

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

4 “(6) coordinating information security policies
5 and procedures with related information resources
6 management policies and procedures;

7 “(7) overseeing the operation of the Federal in-
8 formation security incident center required under sec-
9 tion 3555; and

10 “(8) reporting to Congress no later than March
11 1 of each year on agency compliance with the require-
12 ments of this subchapter, including—

13 “(A) an assessment of the development, pro-
14 mulgation, and adoption of, and compliance
15 with, standards developed under section 20 of the
16 National Institute of Standards and Technology
17 Act (15 U.S.C. 278g-3) and promulgated under
18 section 11331 of title 40;

19 “(B) significant deficiencies in agency in-
20 formation security practices;

21 “(C) planned remedial action to address
22 such deficiencies; and

23 “(D) a summary of, and the views of the
24 Director on, the report prepared by the National
25 Institute of Standards and Technology under

1 *section 20(d)(10) of the National Institute of*
2 *Standards and Technology Act (15 U.S.C. 278g-*
3 *3).*

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

8 “(c) *DEPARTMENT OF DEFENSE AND CENTRAL INTEL-*
9 *LIGENCE AGENCY SYSTEMS.—(1) The authorities of the Di-*
10 *rector described in paragraphs (1) and (2) of subsection (a)*
11 *shall be delegated to the Secretary of Defense in the case*
12 *of systems described in paragraph (2) and to the Director*
13 *of Central Intelligence in the case of systems described in*
14 *paragraph (3).*

15 “(2) *The systems described in this paragraph are sys-*
16 *tems that are operated by the Department of Defense, a con-*
17 *tractor of the Department of Defense, or another entity on*
18 *behalf of the Department of Defense that processes any in-*
19 *formation the unauthorized access, use, disclosure, disrupt-*
20 *tion, modification, or destruction of which would have a*
21 *debilitating impact on the mission of the Department of De-*
22 *fense.*

23 “(3) *The systems described in this paragraph are sys-*
24 *tems that are operated by the Central Intelligence Agency,*
25 *a contractor of the Central Intelligence Agency, or another*

1 *entity on behalf of the Central Intelligence Agency that*
2 *processes any information the unauthorized access, use, dis-*
3 *closure, disruption, modification, or destruction of which*
4 *would have a debilitating impact on the mission of the Cen-*
5 *tral Intelligence Agency.*

6 **“§ 3554. Agency responsibilities**

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

8 “(1) *be responsible for—*

9 “(A) *providing information security protec-*
10 *tions commensurate with the risk and magnitude*
11 *of the harm resulting from unauthorized access,*
12 *use, disclosure, disruption, modification, or de-*
13 *struction of—*

14 “(i) *information collected or main-*
15 *tained by or on behalf of the agency; and*

16 “(ii) *information systems used or oper-*
17 *ated by an agency or by a contractor of an*
18 *agency or other organization on behalf of an*
19 *agency;*

20 “(B) *complying with the requirements of*
21 *this subchapter and related policies, procedures,*
22 *standards, and guidelines, including—*

23 “(i) *information security standards*
24 *and guidelines promulgated under section*
25 *11331 of title 40 and section 20 of the Na-*

1 *tional Institute of Standards and Tech-*
2 *nology Act (15 U.S.C. 278g-3);*

3 *“(ii) information security standards*
4 *and guidelines for national security systems*
5 *issued in accordance with law and as di-*
6 *rected by the President; and*

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

12 *“(C) ensuring that information security*
13 *management processes are integrated with agen-*
14 *cy strategic and operational planning and budg-*
15 *et processes, including policies, procedures, and*
16 *practices described in subsection (c)(2);*

17 *“(D) as appropriate, maintaining secure fa-*
18 *cilities that have the capability of accessing,*
19 *sending, receiving, and storing classified infor-*
20 *mation;*

21 *“(E) maintaining a sufficient number of*
22 *personnel with security clearances, at the appro-*
23 *priate levels, to access, send, receive and analyze*
24 *classified information to carry out the respon-*
25 *sibilities of this subchapter; and*

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

6 “(2) ensure that senior agency officials provide
7 information security for the information and infor-
8 mation systems that support the operations and assets
9 under their control, including through—

10 “(A) assessing the risk and magnitude of
11 the harm that could result from the unauthorized
12 access, use, disclosure, disruption, modification,
13 or destruction of such information or informa-
14 tion system;

15 “(B) determining the levels of information
16 security appropriate to protect such information
17 and information systems in accordance with
18 policies, principles, standards, and guidelines
19 promulgated under section 11331 of title 40 and
20 section 20 of the National Institute of Standards
21 and Technology Act (15 U.S.C. 278g–3) for in-
22 formation security classifications and related re-
23 quirements;

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

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

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

16 “(3) delegate to the Chief Information Officer or
17 equivalent (or a senior agency official who reports to
18 the Chief Information Officer or equivalent), who is
19 designated as the ‘Chief Information Security Officer’,
20 the authority and primary responsibility to develop,
21 implement, and oversee an agencywide information
22 security program to ensure and enforce compliance
23 with the requirements imposed on the agency under
24 this subchapter, including—

1 “(A) overseeing the establishment and main-
2 tenance of a security operations capability that
3 through automated and continuous monitoring,
4 when possible, can—

5 “(i) detect, report, respond to, contain,
6 and mitigate incidents that impair infor-
7 mation security and agency information
8 systems, in accordance with policy provided
9 by the Director;

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

14 “(iii) continually evaluate risks posed
15 to information collected or maintained by
16 or on behalf of the agency and information
17 systems and hold senior agency officials ac-
18 countable for ensuring information security;

19 “(iv) collaborate with the Director and
20 appropriate public and private sector secu-
21 rity operations centers to detect, report, re-
22 spond to, contain, and mitigate incidents
23 that impact the security of information and
24 information systems that extend beyond the
25 control of the agency; and

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

9 “(B) developing, maintaining, and over-
10 seeing an agencywide information security pro-
11 gram as required by subsection (b);

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

17 “(D) training and overseeing personnel
18 with significant responsibilities for information
19 security with respect to such responsibilities; and

20 “(E) assisting senior agency officials con-
21 cerning their responsibilities under paragraph
22 (2);

23 “(4) ensure that the agency has a sufficient num-
24 ber of trained and cleared personnel to assist the
25 agency in complying with the requirements of this

1 *subchapter, other applicable laws, and related poli-*
2 *cies, procedures, standards, and guidelines;*

3 *“(5) ensure that the Chief Information Security*
4 *Officer, in consultation with other senior agency offi-*
5 *cial, reports periodically, but not less than annually,*
6 *to the agency head on—*

7 *“(A) the effectiveness of the agency informa-*
8 *tion security program;*

9 *“(B) information derived from automated*
10 *and continuous monitoring, when possible, and*
11 *threat assessments; and*

12 *“(C) the progress of remedial actions;*

13 *“(6) ensure that the Chief Information Security*
14 *Officer possesses the necessary qualifications, includ-*
15 *ing education, training, experience, and the security*
16 *clearance required to administer the functions de-*
17 *scribed under this subchapter; and has information*
18 *security duties as the primary duty of that official;*
19 *and*

20 *“(7) ensure that components of that agency es-*
21 *tablish and maintain an automated reporting mecha-*
22 *nism that allows the Chief Information Security Offi-*
23 *cer with responsibility for the entire agency, and all*
24 *components thereof, to implement, monitor, and hold*
25 *senior agency officers accountable for the implementa-*

1 *tion of appropriate security policies, procedures, and*
2 *controls of agency components.*

3 “(b) *AGENCY PROGRAM.—Each agency shall develop,*
4 *document, and implement an agencywide information secu-*
5 *rity program, approved by the Director and consistent with*
6 *components across and within agencies, to provide informa-*
7 *tion security for the information and information systems*
8 *that support the operations and assets of the agency, includ-*
9 *ing those provided or managed by another agency, con-*
10 *tractor, or other source, that includes—*

11 “(1) *automated and continuous monitoring,*
12 *when possible, of the risk and magnitude of the harm*
13 *that could result from the disruption or unauthorized*
14 *access, use, disclosure, modification, or destruction of*
15 *information and information systems that support*
16 *the operations and assets of the agency;*

17 “(2) *consistent with guidance developed under*
18 *section 11331 of title 40, vulnerability assessments*
19 *and penetration tests commensurate with the risk*
20 *posed to agency information systems;*

21 “(3) *policies and procedures that—*

22 “(A) *cost effectively reduce information se-*
23 *curity risks to an acceptable level;*

24 “(B) *ensure compliance with—*

1 “(i) the requirements of this sub-
2 chapter;

3 “(ii) policies and procedures as may be
4 prescribed by the Director, and information
5 security standards promulgated pursuant to
6 section 11331 of title 40;

7 “(iii) minimally acceptable system
8 configuration requirements, as determined
9 by the Director; and

10 “(iv) any other applicable require-
11 ments, including—

12 “(I) standards and guidelines for
13 national security systems issued in ac-
14 cordance with law and as directed by
15 the President; and

16 “(II) the National Institute of
17 Standards and Technology standards
18 and guidance;

19 “(C) develop, maintain, and oversee infor-
20 mation security policies, procedures, and control
21 techniques to address all applicable requirements,
22 including those promulgated pursuant section
23 11331 of title 40; and

24 “(D) ensure the oversight and training of
25 personnel with significant responsibilities for in-

1 *formation security with respect to such respon-*
2 *sibilities;*

3 “(4) *with a frequency sufficient to support risk-*
4 *based security decisions, automated and continuous*
5 *monitoring, when possible, for testing and evaluation*
6 *of the effectiveness and compliance of information se-*
7 *curity policies, procedures, and practices, including—*

8 “(A) *controls of every information system*
9 *identified in the inventory required under sec-*
10 *tion 3505(c); and*

11 “(B) *controls relied on for an evaluation*
12 *under this section;*

13 “(5) *a process for planning, implementing, eval-*
14 *uating, and documenting remedial action to address*
15 *any deficiencies in the information security policies,*
16 *procedures, and practices of the agency;*

17 “(6) *with a frequency sufficient to support risk-*
18 *based security decisions, automated and continuous*
19 *monitoring, when possible, for detecting, reporting,*
20 *and responding to security incidents, consistent with*
21 *standards and guidelines issued by the National In-*
22 *stitute of Standards and Technology, including—*

23 “(A) *mitigating risks associated with such*
24 *incidents before substantial damage is done;*

1 “(B) notifying and consulting with the Fed-
2 eral information security incident center and
3 other appropriate security operations response
4 centers; and

5 “(C) notifying and consulting with, as ap-
6 propriate—

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

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

12 “(7) plans and procedures to ensure continuity
13 of operations for information systems that support the
14 operations and assets of the agency.

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

16 “(1) submit an annual report on the adequacy
17 and effectiveness of information security policies, pro-
18 cedures, and practices, and compliance with the re-
19 quirements of this subchapter, including compliance
20 with each requirement of subsection (b) to—

21 “(A) the Director;

22 “(B) the Committee on Homeland Security
23 and Governmental Affairs of the Senate;

24 “(C) the Committee on Oversight and Gov-
25 ernment Reform of the House of Representatives;

1 “(D) other appropriate authorization and
2 appropriations committees of Congress; and

3 “(E) the Comptroller General;

4 “(2) address the adequacy and effectiveness of in-
5 formation security policies, procedures, and practices
6 in plans and reports relating to—

7 “(A) annual agency budgets;

8 “(B) information resources management of
9 this subchapter;

10 “(C) information technology management
11 under this chapter;

12 “(D) program performance under sections
13 1105 and 1115 through 1119 of title 31, and sec-
14 tions 2801 and 2805 of title 39;

15 “(E) financial management under chapter
16 9 of title 31, and the Chief Financial Officers
17 Act of 1990 (31 U.S.C. 501 note; Public Law
18 101–576);

19 “(F) financial management systems under
20 the Federal Financial Management Improvement
21 Act of 1996 (31 U.S.C. 3512 note); and

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

1 “(3) report any significant deficiency in a pol-
2 icy, procedure, or practice identified under paragraph
3 (1) or (2)—

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

6 “(B) if relating to financial management
7 systems, as an instance of a lack of substantial
8 compliance under the Federal Financial Man-
9 agement Improvement Act of 1996 (31 U.S.C.
10 3512 note).

11 **“§ 3555. Federal information security incident center**

12 “(a) *IN GENERAL.*—The Director shall ensure the oper-
13 ation of a central Federal information security incident
14 center to—

15 “(1) provide timely technical assistance to opera-
16 tors of agency information systems regarding security
17 incidents, including guidance on detecting and han-
18 dling information security incidents;

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

21 “(3) inform operators of agency information sys-
22 tems about current and potential information secu-
23 rity threats, and vulnerabilities; and

24 “(4) consult with the National Institute of
25 Standards and Technology, agencies or offices oper-

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

6 “(b) *NATIONAL SECURITY SYSTEMS.—Each agency op-*
7 *erating or exercising control of a national security system*
8 *shall share information about information security inci-*
9 *dents, threats, and vulnerabilities with the Federal informa-*
10 *tion security incident center to the extent consistent with*
11 *standards and guidelines for national security systems,*
12 *issued in accordance with law and as directed by the Presi-*
13 *dent.*

14 “(c) *REVIEW AND APPROVAL.—The Director shall re-*
15 *view and approve the policies, procedures, and guidance es-*
16 *tablished in this subchapter to ensure that the incident cen-*
17 *ter has the capability to effectively and efficiently detect,*
18 *correlate, respond to, contain, mitigate, and remediate inci-*
19 *dents that impair the adequate security of the information*
20 *systems of more than one agency. To the extent practicable,*
21 *the capability shall be continuous and technically auto-*
22 *mated.*

1 **“§ 3556. National security systems**

2 *“The head of each agency operating or exercising con-*
 3 *trol of a national security system shall be responsible for*
 4 *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, dis-*
 8 *closure, disruption, modification, or destruction of the*
 9 *information contained in such system;*

10 *“(2) implements information security policies*
 11 *and practices as required by standards and guidelines*
 12 *for national security systems, issued in accordance*
 13 *with law and as directed by the President; and*

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

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

17 *(a) TABLE OF SECTIONS IN TITLE 44.—The table of*
 18 *sections for chapter 35 of title 44, United States Code, is*
 19 *amended by striking the matter relating to subchapters II*
 20 *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.”.

21 *(b) OTHER REFERENCES.—*

1 (1) *Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended*
2
3 *by striking “section 3532(3)” and inserting “section*
4 *3552(b)”.*

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

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

11 (4) *Section 2315 of title 10, United States Code,*
12 *is amended by striking “section 3542(b)(2)” and in-*
13 *serting “section 3552(b)”.*

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

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

20 (B) *in subsection (e)(2), by striking “section*
21 *3532(1)” and inserting “section 3552(b)”.*

22 (6) *Section 8(d)(1) of the Cyber Security Re-*
23 *search and Development Act (15 U.S.C. 7406(d)(1)) is*
24 *amended by striking “section 3534(b)” and inserting*
25 *“section 3554(b)”.*

1 **SEC. 4. EFFECTIVE DATE.**

2 *This Act (including the amendments made by this Act)*
3 *shall take effect 30 days after the date of the enactment of*
4 *this Act.*

Union Calendar No. 318

112TH CONGRESS
2^D SESSION

H. R. 4257

[Report No. 112-455]

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 26, 2012

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