

112TH CONGRESS
2D SESSION

H. R. 4257

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

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 2012”.

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:

1 “SUBCHAPTER II—INFORMATION SECURITY

2 “§ 3551. **Purposes**

3 “The purposes of this subchapter are to—

4 “(1) provide a comprehensive framework for en-
5 suring the effectiveness of information security con-
6 trols over information resources that support Fed-
7 eral operations and assets;

8 “(2) recognize the highly networked nature of
9 the current Federal computing environment and pro-
10 vide effective Governmentwide management and
11 oversight of the related information security risks,
12 including coordination of information security efforts
13 throughout the civilian, national security, and law
14 enforcement communities assets;

15 “(3) provide for development and maintenance
16 of minimum controls required to protect Federal in-
17 formation and information infrastructure;

18 “(4) provide a mechanism for improved over-
19 sight of Federal agency information security pro-
20 grams and systems through a focus on automated
21 and continuous monitoring of agency information
22 systems and regular threat assessments;

23 “(5) acknowledge that commercially developed
24 information security products offer advanced, dy-
25 namic, robust, and effective information security so-

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

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

10 **“§ 3552. Definitions**

11 “(a) SECTION 3502 DEFINITIONS.—Except as pro-
12 vided under subsection (b), the definitions under section
13 3502 shall apply to this subchapter.

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

15 “(1) The term ‘adequate security’ means secu-
16 rity that complies with the regulations and stand-
17 ards promulgated under section 11331 of title 40.

18 “(2) The term ‘automated and continuous mon-
19 itoring’ means monitoring, with minimal human in-
20 volvement, through an uninterrupted, ongoing real-
21 time, or near real-time process used to determine if
22 the complete set of planned, required, and deployed
23 security controls within an information system con-
24 tinue to be effective over time with rapidly changing
25 information technology and threat development.

1 “(3) The term ‘incident’ means an occurrence
2 that actually or potentially jeopardizes the confiden-
3 tiality, integrity, or availability of an information
4 system, information infrastructure, or the informa-
5 tion the system processes, stores, or transmits or
6 that constitutes a violation or imminent threat of
7 violation of security policies, security procedures, or
8 acceptable use policies.

9 “(4) The term ‘information infrastructure’
10 means the underlying framework that information
11 systems and assets rely on in processing, storing, or
12 transmitting information electronically.

13 “(5) The term ‘information security’ means
14 protecting information and information infrastruc-
15 ture from unauthorized access, use, disclosure, dis-
16 ruption, modification, or destruction in order to pro-
17 vide—

18 “(A) integrity, which means guarding
19 against improper information modification or
20 destruction, and includes ensuring information
21 nonrepudiation and authenticity;

22 “(B) confidentiality, which means pre-
23 serving authorized restrictions on access and
24 disclosure, including means for protecting per-
25 sonal privacy and proprietary information;

1 “(C) availability, which means ensuring
2 timely and reliable access to and use of infor-
3 mation; and

4 “(D) authentication, which means using
5 digital credentials to assure the identity of
6 users and validate access of such users.

7 “(6) The term ‘information technology’ has the
8 meaning given that term in section 11101 of title
9 40.

10 “(7)(A) The term ‘national security system’
11 means any information infrastructure (including any
12 telecommunications system) used or operated by an
13 agency or by a contractor of an agency, or other or-
14 ganization on behalf of an agency—

15 “(i) the function, operation, or use of
16 which—

17 “(I) involves intelligence activities;

18 “(II) involves cryptologic activities re-
19 lated to national security;

20 “(III) involves command and control
21 of military forces;

22 “(IV) involves equipment that is an
23 integral part of a weapon or weapons sys-
24 tem; or

1 “(V) subject to subparagraph (B), is
2 critical to the direct fulfillment of military
3 or intelligence missions; or

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

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

14 “(8) The term ‘information system’ means any
15 equipment or interconnected system or subsystem of
16 equipment that is used in the automatic acquisition,
17 storage, manipulation, management, movement, con-
18 trol, display, switching, interchange, transmission, or
19 reception of data or information, and includes—

20 “(A) computers and computer networks;

21 “(B) ancillary equipment;

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

24 “(D) services, including support services;

25 and

1 “(E) related resources.

2 “(9) The term ‘threat assessment’ means the
3 real-time or near real-time process of formally evalu-
4 ating the degree of threat to an information system
5 or information technology enterprise and describing
6 the nature of the threat.

7 **“§ 3553. Authority and functions of the Director**

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

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

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

23 “(A) information collected or maintained
24 by or on behalf of an agency; or

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

4 “(3) coordinating the development of standards
5 and guidelines under section 20 of the National In-
6 stitute of Standards and Technology Act (15 U.S.C.
7 278g–3) with agencies and offices operating or exer-
8 cising control of national security systems (including
9 the National Security Agency) to assure, to the max-
10 imum extent feasible, that such standards and
11 guidelines are complementary with standards and
12 guidelines developed for national security systems;

13 “(4) overseeing agency compliance with the re-
14 quirements of this subchapter, including through
15 any authorized action under section 11303 of title
16 40, to enforce accountability for compliance with
17 such requirements;

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

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

1 “(7) overseeing the operation of the Federal in-
2 formation security incident center required under
3 section 3555; and

4 “(8) reporting to Congress no later than March
5 1 of each year on agency compliance with the re-
6 quirements of this subchapter, including—

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

13 “(B) significant deficiencies in agency in-
14 formation security practices;

15 “(C) planned remedial action to address
16 such deficiencies; and

17 “(D) a summary of, and the views of the
18 Director on, the report prepared by the Na-
19 tional Institute of Standards and Technology
20 under section 20(d)(10) of the National Insti-
21 tute of Standards and Technology Act (15
22 U.S.C. 278g–3).

23 “(b) NATIONAL SECURITY SYSTEMS.—Except for the
24 authorities described in paragraphs (4) and (8) of sub-

1 section (a), the authorities of the Director under this sec-
2 tion shall not apply to national security systems.

3 “(c) DEPARTMENT OF DEFENSE AND CENTRAL IN-
4 TELLIGENCE AGENCY SYSTEMS.—(1) The authorities of
5 the Director described in paragraphs (1) and (2) of sub-
6 section (a) shall be delegated to the Secretary of Defense
7 in the case of systems described in paragraph (2) and to
8 the Director of Central Intelligence in the case of systems
9 described in paragraph (3).

10 “(2) The systems described in this paragraph
11 are systems that are operated by the Department of
12 Defense, a contractor of the Department of Defense,
13 or another entity on behalf of the Department of
14 Defense that processes any information the unau-
15 thorized access, use, disclosure, disruption, modifica-
16 tion, or destruction of which would have a debili-
17 tating impact on the mission of the Department of
18 Defense.

19 “(3) The systems described in this paragraph
20 are systems that are operated by the Central Intel-
21 ligence Agency, a contractor of the Central Intel-
22 ligence Agency, or another entity on behalf of the
23 Central Intelligence Agency that processes any infor-
24 mation the unauthorized access, use, disclosure, dis-
25 ruption, modification, or destruction of which would

1 have a debilitating impact on the mission of the Cen-
2 tral Intelligence Agency.

3 **“§ 3554. 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 infrastructure used
14 or operated by an agency or by a con-
15 tractor of an agency or other organization
16 on behalf 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 policies,
21 principles, standards, and guidelines pro-
22 mulgated under section 11331 of title 40
23 and section 20 of the National Institute of
24 Standards and Technology Act (15 U.S.C.
25 278g–3);

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

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

10 “(C) ensuring that information security
11 management processes are integrated with
12 agency strategic and operational planning and
13 budget processes, including policies, procedures,
14 and practices described in subsection (c)(2);

15 “(D) as appropriate, maintaining secure
16 facilities that have the capability of accessing,
17 sending, receiving, and storing classified infor-
18 mation;

19 “(E) maintaining a sufficient number of
20 personnel with security clearances, at the ap-
21 propriate levels, to access, send, receive and
22 analyze classified information to carry out the
23 responsibilities of this subchapter; and

24 “(F) ensuring that information security
25 performance indicators and measures are in-

1 cluded in the annual performance evaluations of
2 all managers, senior managers, senior executive
3 service personnel, and political appointees;

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

8 “(A) assessing the risk and magnitude of
9 the harm that could result from the unauthor-
10 ized access, use, disclosure, disruption, modi-
11 fication, or destruction of such information or
12 information infrastructure;

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

22 “(C) implementing policies and procedures
23 to cost effectively reduce risks to an acceptable
24 level;

1 “(D) with a frequency commensurate with
2 the risk to information security, continuously
3 testing and evaluating information security con-
4 trols and techniques to ensure that such con-
5 trols and techniques are effectively implemented
6 and operated; and

7 “(E) with a frequency commensurate with
8 the risk to information security, continuously
9 conducting threat assessments by monitoring
10 information infrastructure, identifying potential
11 system vulnerabilities, and reporting security
12 incidents in accordance with paragraph
13 (3)(A)(v);

14 “(3) delegate to the Chief Information Officer
15 or equivalent (or a senior agency official who reports
16 to the Chief Information Officer or equivalent), who
17 is designated as the ‘Chief Information Security Of-
18 ficer’, the authority and primary responsibility to de-
19 velop, implement, and oversee an agencywide infor-
20 mation security program to ensure and enforce com-
21 pliance with the requirements imposed on the agency
22 under this subchapter, including—

23 “(A) overseeing the establishment and
24 maintenance of a security operations capability

1 that through automated and continuous moni-
2 toring can—

3 “(i) detect, report, respond to, con-
4 tain, and mitigate incidents that impair in-
5 formation security, information systems,
6 and agency information infrastructure, in
7 accordance with policy provided by the Di-
8 rector;

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

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
18 accountable for ensuring information secu-
19 rity;

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

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

3 “(v) report any incident described
4 under clauses (i) and (ii) to the appro-
5 priate security operations center and the
6 Inspector General of the agency, to the ex-
7 tent practicable, within 24 hours after dis-
8 covery of the incident, but no later than 48
9 hours after such discovery;

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

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

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

22 “(E) assisting senior agency officials con-
23 cerning their responsibilities under paragraph
24 (2);

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

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

10 “(A) the effectiveness of the agency infor-
11 mation security program;

12 “(B) information derived from automated
13 and continuous monitoring and threat assess-
14 ments; and

15 “(C) the progress of remedial actions;

16 “(6) ensure that the Chief Information Security
17 Officer possesses the necessary qualifications, includ-
18 ing education, professional certifications, training,
19 experience, and the security clearance required to
20 administer the functions described under this sub-
21 chapter; and has information security duties as the
22 primary duty of that official;

23 “(7) ensure that components of that agency es-
24 tablish and maintain an automated reporting mecha-
25 nism that allows the Chief Information Security Of-

1 ficer with responsibility for the entire agency, and all
2 components thereof, to implement, monitor, and hold
3 senior agency officers accountable for the implemen-
4 tation of appropriate security policies, procedures,
5 and controls of agency components; and

6 “(8) delegate to agency officials who are re-
7 sponsible for particular agency systems or sub-
8 systems the responsibility to ensure and enforce
9 compliance with all requirements of the agency’s in-
10 formation security program in consultation with the
11 Chief Information Security Officer designated under
12 paragraph (3).

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

21 “(1) automated and continuous monitoring—

22 “(A) of the risk and magnitude of the
23 harm that could result from the disruption or
24 unauthorized access, use, disclosure, modifica-
25 tion, or destruction of information and informa-

1 tion systems that support the operations and
2 assets of the agency; and

3 “(B) that assesses whether information or
4 information systems should be removed or mi-
5 grated to more secure networks or standards
6 and make recommendations to the head of the
7 agency and the Director based on that assess-
8 ment;

9 “(2) consistent with guidance developed under
10 section 11331 of title 40, vulnerability assessments
11 and penetration tests commensurate with the risk
12 posed to an agency information infrastructure;

13 “(3) policies and procedures that—

14 “(A) mitigate and, to the extent prac-
15 ticable, remediate information security
16 vulnerabilities based on the risk posed to the
17 agency;

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

20 “(C) ensure compliance with—

21 “(i) the requirements of this sub-
22 chapter;

23 “(ii) policies and procedures as may
24 be prescribed by the Director, and infor-

1 mation security standards promulgated
2 pursuant to section 11331 of title 40;

3 “(iii) minimally acceptable system
4 configuration requirements, as determined
5 by the Director; and

6 “(iv) any other applicable require-
7 ments, including—

8 “(I) standards and guidelines for
9 national security systems issued in ac-
10 cordance with law and as directed by
11 the President;

12 “(II) the National Institute of
13 Standards and Technology guidance;
14 and

15 “(III) the Chief Information Offi-
16 cers Council recommended ap-
17 proaches;

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

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

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

3 “(4) consistent with the risk to information se-
4 curity, automated and continuous monitoring for
5 testing, and evaluation of the effectiveness and com-
6 pliance of information security policies, procedures,
7 and practices, including—

8 “(A) management, operational, and tech-
9 nical controls of every information system iden-
10 tified in the inventory required under section
11 3505(c); and

12 “(B) management, operational, and tech-
13 nical controls relied on for an evaluation under
14 this section;

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

19 “(6) consistent with the risk to information se-
20 curity, automated and continuous monitoring for de-
21 tecting, reporting, and responding to security inci-
22 dents, consistent with standards and guidelines
23 issued by the Director, including—

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

1 “(B) notifying and consulting with the ap-
2 propriate security operations response center;
3 and

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

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

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

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

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

15 “(1) submit an annual report on the adequacy
16 and effectiveness of information security policies,
17 procedures, and practices, and compliance with the
18 requirements of this subchapter, including compli-
19 ance with each requirement of subsection (b) to—

20 “(A) the Director;

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

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

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
5 information security policies, procedures, and prac-
6 tices 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
14 sections 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 Improve-
21 ment 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 para-
3 graph (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
13 operation of a central Federal information security inci-
14 dent center to—

15 “(1) provide timely technical assistance to oper-
16 ators of agency information systems and information
17 infrastructure regarding security incidents, including
18 guidance on detecting and handling information se-
19 curity incidents;

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

22 “(3) inform operators of agency information
23 systems and information infrastructure about cur-
24 rent and potential information security threats, and
25 vulnerabilities; and

1 “(4) 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 “(c) REVIEW AND APPROVAL.—The Director shall
17 review and approve the policies, procedures, and guidance
18 established in this subchapter to ensure that the incident
19 center has the capability to effectively and efficiently de-
20 tect, correlate, respond to, contain, mitigate, and reme-
21 diate incidents that impair the adequate security of the
22 information systems and information infrastructure of
23 more than one agency. To the extent practicable, the capa-
24 bility shall be continuous and technically automated.

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

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

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

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

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

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

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

“SUBCHAPTER II—INFORMATION SECURITY

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

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

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

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

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

20 (B) in subsection (e)(2), by striking “sec-
21 tion 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))
24 is amended by striking “section 3534(b)” and in-
25 serting “section 3554(b)”.

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

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

○