

111TH CONGRESS
2^D SESSION

H. R. 4900

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 22, 2010

Ms. WATSON 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 create the National Office for Cyberspace, 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 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Federal Information Security Amendments Act of
6 2010”.

7 (b) **TABLE OF CONTENTS.**—The table of contents for
8 this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Coordination of Federal Information Policy.
- Sec. 3. Information Security Acquisition Requirements.
- Sec. 4. Technical and conforming amendments.
- Sec. 5. Effective date.

1 **SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-**
2 **ICY.**

3 Chapter 35 of title 44, United States Code, is amend-
4 ed by striking subchapters II and III and inserting the
5 following:

6 “SUBCHAPTER II—INFORMATION SECURITY

7 “§ 3551. **Purposes**

8 “The purposes of this subchapter are to—

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

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

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

1 “(4) provide a mechanism for improved over-
2 sight of Federal agency information security pro-
3 grams;

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

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

16 **“§ 3552. Definitions**

17 “(a) SECTION 3502 DEFINITIONS.—Except as pro-
18 vided under subsection (b), the definitions under section
19 3502 shall apply to this subchapter.

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

21 “(1) The term ‘adequate security’ means secu-
22 rity that complies with the regulations promulgated
23 under section 3554 and the standards promulgated
24 under section 3558.

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

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

12 “(4) The term ‘information security’ means
13 protecting information and information systems
14 from unauthorized access, use, disclosure, disrup-
15 tion, modification, or destruction in order to pro-
16 vide—

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

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

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

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

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

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

14 “(I) involves intelligence activities;

15 “(II) involves cryptologic activities re-
16 lated to national security;

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

19 “(IV) involves equipment that is an
20 integral part of a weapon or weapons sys-
21 tem; or

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

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

7 “(B) Subparagraph (A)(I)(V) does not include
8 a system that is to be used for routine administra-
9 tive and business applications (including payroll, fi-
10 nance, logistics, and personnel management applica-
11 tions).

12 **“§ 3553. National Office for Cyberspace**

13 “(a) ESTABLISHMENT.—There is established within
14 the Executive Office of the President an office to be known
15 as the National Office for Cyberspace.

16 “(b) DIRECTOR.—There shall be at the head of the
17 Office a Director, who shall be appointed by the President
18 by and with the advice and consent of the Senate. The
19 Director of the National Office for Cyberspace shall ad-
20 minister all functions under this subchapter and collabo-
21 rate to the extent practicable with the heads of appro-
22 priate agencies, the private sector, and international part-
23 ners. The Office shall serve as the principal office for co-
24 ordinating issues relating to achieving an assured, reliable,

1 secure, and survivable information infrastructure and re-
2 lated capabilities for the Federal Government.

3 **“§ 3554. Federal Cybersecurity Practice Board**

4 “(a) ESTABLISHMENT.—Within the National Office
5 for Cyberspace, there shall be established a board to be
6 known as the ‘Federal Cybersecurity Practice Board’ (in
7 this section referred to as the ‘Board’).

8 “(b) MEMBERS.—The Board shall be chaired by the
9 Director of the National Office for Cyberspace and consist
10 of at least one representative from—

11 “(1) the Office of Management and Budget;

12 “(2) civilian agencies;

13 “(3) the Department of Defense;

14 “(4) the law enforcement community; and

15 “(5) such additional military and civilian agen-
16 cies as the Director considers appropriate.

17 “(c) RESPONSIBILITIES.—

18 “(1) DEVELOPMENT OF POLICIES AND PROCE-
19 DURES.—Subject to the authority, direction, and
20 control of the Director of the National Office for
21 Cyberspace, the Board shall be responsible for devel-
22 oping and periodically updating information security
23 policies and procedures relating to the matters de-
24 scribed in paragraph (2). In developing such policies
25 and procedures, the Board shall require that all

1 matters addressed in the policies and procedures are
2 consistent, to the maximum extent practicable and
3 in accordance with applicable law, among the civil-
4 ian, military, intelligence, and law enforcement com-
5 munities.

6 “(2) SPECIFIC MATTERS COVERED IN POLICIES
7 AND PROCEDURES.—

8 “(A) MINIMUM SECURITY CONTROLS.—

9 The Board shall be responsible for developing
10 and periodically updating information security
11 policies and procedures relating to minimum se-
12 curity controls for information technology, in
13 order to—

14 “(i) provide Governmentwide protec-
15 tion of Government-networked computers
16 against common attacks; and

17 “(ii) provide agencywide protection
18 against threats, vulnerabilities, and other
19 risks to the information infrastructure
20 within individual agencies.

21 “(B) MEASURES OF EFFECTIVENESS.—

22 The Board shall be responsible for developing
23 and periodically updating information security
24 policies and procedures relating to measure-
25 ments needed to assess the effectiveness of the

1 minimum security controls referred to in sub-
2 paragraph (A). Such measurements shall in-
3 clude a risk scoring system to evaluate risk to
4 information security both Governmentwide and
5 within contractors of the Federal Government.

6 “(C) PRODUCTS AND SERVICES.—The
7 Board shall be responsible for developing and
8 periodically updating information security poli-
9 cies and procedures relating to criteria for prod-
10 ucts and services to be used in agency informa-
11 tion systems and agency information infrastruc-
12 ture that will meet the minimum security con-
13 trols referred to in subparagraph (A). In car-
14 rying out this subparagraph, the Board shall, in
15 consultation with the Office of Management
16 and Budget and the General Services Adminis-
17 tration—

18 “(i) develop a list, set forth in order
19 of priority, of technologies that agencies
20 can use to automate security functions;
21 and

22 “(ii) define minimum standards for
23 secure development of software products
24 and services.

1 “(D) REMEDIES.—The Board shall be re-
2 sponsible for developing and periodically updat-
3 ing information security policies and procedures
4 relating to methods for providing remedies for
5 security deficiencies identified in agency infor-
6 mation systems.

7 “(3) RELATIONSHIP TO OTHER STANDARDS.—
8 The policies and procedures developed under para-
9 graph (1) are supplemental to the standards promul-
10 gated by the Director of the National Office for
11 Cyberspace under section 3558.

12 “(4) RECOMMENDATIONS FOR REGULATIONS.—
13 The Board shall be responsible for making rec-
14 ommendations to the Director of the National Office
15 for Cyberspace on regulations to carry out the poli-
16 cies and procedures developed by the Board under
17 paragraph (1).

18 “(d) REGULATIONS.—The Director of the National
19 Office for Cyberspace, in consultation with the Director
20 of the Office of Management and the Administrator of
21 General Services, shall promulgate and periodically update
22 regulations to carry out the policies and procedures devel-
23 oped by the Board under subsection (c).

24 “(e) ANNUAL REPORT.—The Director of the Na-
25 tional Office for Cyberspace shall provide to Congress a

1 report containing a summary of agency progress in imple-
2 menting the regulations promulgated under this section as
3 part of the annual report to Congress required under sec-
4 tion 3555(a)(8).

5 “(f) EXEMPTION FROM DISCLOSURE.—Information
6 regarding threats, vulnerabilities, and risks submitted by
7 agencies to the Board shall be exempt from disclosure
8 under section 552 of title 5.

9 **“§ 3555. Authority and functions of the Director of**
10 **the National Office for Cyberspace**

11 “(a) IN GENERAL.—The Director of the National Of-
12 fice for Cyberspace shall oversee agency information secu-
13 rity policies and practices, including—

14 “(1) developing and overseeing the implementa-
15 tion of policies, principles, standards, and guidelines
16 on information security, including through ensuring
17 timely agency adoption of and compliance with
18 standards promulgated under section 3558;

19 “(2) requiring agencies, consistent with the
20 standards promulgated under section 3558 and
21 other requirements of this subchapter, to identify
22 and provide information security protections com-
23 mensurate with the risk and magnitude of the harm
24 resulting from the unauthorized access, use, disclo-
25 sure, disruption, modification, or destruction of—

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

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

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

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

20 “(5) reviewing at least annually, and approving
21 or disapproving, agency information security pro-
22 grams required under section 3556(b);

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

1 “(7) overseeing the operation of the Federal in-
2 formation security incident center required under
3 section 3559; 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) a summary of the findings of audits
8 required by section 3557;

9 “(B) an assessment of the development,
10 promulgation, and adoption of, and compliance
11 with, standards developed under section 20 of
12 the National Institute of Standards and Tech-
13 nology Act (15 U.S.C. 278g–3) and promul-
14 gated under section 3558;

15 “(C) significant deficiencies in agency in-
16 formation security practices;

17 “(D) planned remedial action to address
18 such deficiencies; and

19 “(E) a summary of, and the views of the
20 Director of the National Office for Cyberspace
21 on, the report prepared by the National Insti-
22 tute of Standards and Technology under section
23 20(d)(10) of the National Institute of Stand-
24 ards and Technology Act (15 U.S.C. 278g–3).

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

6 “(c) DEPARTMENT OF DEFENSE AND CENTRAL IN-
7 TELLIGENCE AGENCY SYSTEMS.—(1) The authorities of
8 the Director of the National Office for Cyberspace de-
9 scribed in paragraphs (1) and (2) of subsection (a) shall
10 be delegated to the Secretary of Defense in the case of
11 systems described in paragraph (2) and to the Director
12 of Central Intelligence in the case of systems described
13 in paragraph (3).

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

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

1 processes any information the unauthorized access, use,
2 disclosure, disruption, modification, or destruction of
3 which would have a debilitating impact on the mission of
4 the Central Intelligence Agency.

5 **“§ 3556. Agency responsibilities**

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

7 “(1) be responsible for—

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

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

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

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

22 “(i) the regulations promulgated
23 under section 3554 and the information se-
24 curity standards promulgated under sec-
25 tion 3558;

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 under the agency
8 head are complementary and uniform, to
9 the extent practicable; and

10 “(C) ensuring that information security
11 management processes are integrated with
12 agency strategic and operational planning pro-
13 cesses;

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

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

23 “(B) determining the levels of information
24 security appropriate to protect such information
25 and information systems in accordance with

1 regulations promulgated under section 3554
2 and standards promulgated under section 3558,
3 for information security classifications and re-
4 lated requirements;

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

8 “(D) continuously testing and evaluating
9 information security controls and techniques to
10 ensure that they are effectively implemented;

11 “(3) delegate to an agency official designated to
12 oversee agency information security the authority to
13 ensure and enforce compliance with the require-
14 ments imposed on the agency under this subchapter,
15 including—

16 “(A) overseeing the establishment and
17 maintenance of a security operations capability
18 on an automated and continuous basis that
19 can—

20 “(i) assess the state of compliance of
21 all networks and systems with prescribed
22 controls issued pursuant to section 3558
23 and report immediately any variance there-
24 from and, where appropriate, shut down

1 systems that are found to be non-compli-
2 ant;

3 “(ii) detect, report, respond to, con-
4 tain, and mitigate incidents that impair
5 adequate security of the information and
6 information infrastructure, in accordance
7 with policy provided by the Director of the
8 National Office for Cyberspace, in con-
9 sultation with the Chief Information Offi-
10 cers Council, and guidance from the Na-
11 tional Institute of Standards and Tech-
12 nology;

13 “(iii) collaborate with the National
14 Office for Cyberspace and appropriate pub-
15 lic and private sector security operations
16 centers to address incidents that impact
17 the security of information and informa-
18 tion infrastructure that extend beyond the
19 control of the agency; and

20 “(iv) not later than 24 hours after
21 discovery of any incident described under
22 subparagraph (A (ii)), unless otherwise di-
23 rected by policy of the National Office for
24 Cyberspace, provide notice to the appro-
25 priate security operations center, the Na-

1 tional Cyber Investigative Joint Task
2 Force, and inspector general;

3 “(B) developing, maintaining, and over-
4 seeing an agency wide information security pro-
5 gram as required by subsection (b);

6 “(C) developing, maintaining, and over-
7 seeing information security policies, procedures,
8 and control techniques to address all applicable
9 requirements, including those issued under sec-
10 tions 3555 and 3558;

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

15 “(E) assisting senior agency officials con-
16 cerning their responsibilities under paragraph
17 (2);

18 “(4) ensure that the agency has trained and
19 cleared personnel sufficient to assist the agency in
20 complying with the requirements of this subchapter
21 and related policies, procedures, standards, and
22 guidelines;

23 “(5) ensure that the agency official designated
24 to oversee agency information security, in coordina-
25 tion with other senior agency officials, reports bian-

1 nually to the agency head on the effectiveness of the
2 agency information security program, including
3 progress of remedial actions; and

4 “(6) ensure that the agency official designated
5 to oversee agency information security possesses nec-
6 essary qualifications, including education, profes-
7 sional certifications, training, experience, and the se-
8 curity clearance required to administer the functions
9 described under this subchapter; and has informa-
10 tion security duties as the primary duty of that offi-
11 cial.

12 “(b) AGENCY PROGRAM.—Each agency shall develop,
13 document, and implement an agencywide information se-
14 curity program, approved by the Director of the National
15 Office for Cyberspace under section 3555(a)(5), to provide
16 information security for the information and information
17 systems that support the operations and assets of the
18 agency, including those provided or managed by another
19 agency, contractor, or other source, that includes—

20 “(1) continuous automated monitoring of infor-
21 mation systems used or operated by an agency or by
22 a contractor of an agency or other organization on
23 behalf of an agency to assure conformance with reg-
24 ulations promulgated under section 3554 and stand-
25 ards promulgated under section 3558;

1 “(2) penetration tests commensurate with risk
2 (as defined by the National Institute of Standards
3 and Technology and the National Office for Cyber-
4 space) for agency information systems;

5 “(3) information security vulnerabilities are
6 mitigated based on the risk posed to the agency;

7 “(4) policies and procedures that—

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

10 “(B) ensure that information security is
11 addressed throughout the life cycle of each
12 agency information system; and

13 “(C) ensure compliance with—

14 “(i) the requirements of this sub-
15 chapter;

16 “(ii) policies and procedures as may
17 be prescribed by the Director of the Na-
18 tional Office for Cyberspace, and informa-
19 tion security standards promulgated under
20 section 3558;

21 “(iii) minimally acceptable system
22 configuration requirements, as determined
23 by the Director of the National Office for
24 Cyberspace; and

1 “(iv) any other applicable require-
2 ments, including standards and guidelines
3 for national security systems issued in ac-
4 cordance with law and as directed by the
5 President; of how the controls described
6 under subparagraph (A) maintain the ap-
7 propriate level of confidentiality, integrity,
8 and availability of information and infor-
9 mation systems based on—

10 “(I) the policy of the Director of
11 the National Office for Cyberspace;

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) developing, maintaining, and over-
19 seeing an agency wide information security pro-
20 gram as required by subsection (b);

21 “(E) developing, maintaining, and over-
22 seeing information security policies, procedures,
23 and control techniques to address all applicable
24 requirements, including those issued under sec-
25 tions 3555 and 3558;

1 “(F) training and overseeing personnel
2 with significant responsibilities for information
3 security with respect to such responsibilities;
4 and

5 “(G) assisting senior agency officials con-
6 cerning their responsibilities under paragraph
7 (2);

8 “(5) ensure that the agency has trained and
9 cleared personnel sufficient to assist the agency in
10 complying with the requirements of this subchapter
11 and related policies, procedures, standards, and
12 guidelines;

13 “(6) ensure that the agency official designated
14 to oversee agency information security, in coordina-
15 tion with other senior agency officials, reports bian-
16 nually to the agency head on the effectiveness of the
17 agency information security program, including
18 progress of remedial actions; and

19 “(7) ensure that the agency official designated
20 to oversee agency information security possesses nec-
21 essary qualifications, including education, profes-
22 sional certifications, training, experience, and the se-
23 curity clearance required to administer the functions
24 described under this subchapter; and has informa-

1 tion security duties as the primary duty of that offi-
2 cial.

3 “(8) to the extent practicable, automated and
4 continuous technical monitoring for testing, and
5 evaluation of the effectiveness and compliance of in-
6 formation security policies, procedures, and prac-
7 tices, 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(b); and

12 “(B) management, operational, and tech-
13 nical controls relied on for an evaluation under
14 section 3556;

15 “(9) 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 “(10) to the extent practicable, continuous tech-
20 nical monitoring for detecting, reporting, and re-
21 sponding to security incidents, consistent with stand-
22 ards and guidelines issued by the Director of the
23 National Office for Cyberspace, 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;

8 “(ii) the National Office for Cyber-
9 space; and

10 “(iii) any other agency or office, in ac-
11 cordance with law or as directed by the
12 President; and

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

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

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

22 “(A) the National Office for Cyberspace;

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

1 “(C) the Committee on Oversight and Gov-
2 ernment Reform of the House of Representa-
3 tives;

4 “(D) other appropriate authorization and
5 appropriations committees of Congress; and

6 “(E) the Comptroller General;

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

10 “(A) annual agency budgets;

11 “(B) information resources management of
12 this subchapter;

13 “(C) information technology management
14 under this chapter;

15 “(D) program performance under sections
16 1105 and 1115 through 1119 of title 31, and
17 sections 2801 and 2805 of title 39;

18 “(E) financial management under chapter
19 9 of title 31, and the Chief Financial Officers
20 Act of 1990 (31 U.S.C. 501 note; Public Law
21 101–576) (and the amendments made by that
22 Act);

23 “(F) financial management systems under
24 the Federal Financial Management Improve-
25 ment Act (31 U.S.C. 3512 note); and

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

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

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

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

13 “(d) PERFORMANCE PLAN.—(1) In addition to the
14 requirements of subsection(c), each agency, in consulta-
15 tion with the National Office for Cyberspace, shall include
16 as part of the performance plan required under section
17 1115 of title 31 a description of—

18 “(A) the time periods; and

19 “(B) the resources, including budget, staff-
20 ing, and training, that are necessary to imple-
21 ment the program required under subsection
22 (b).

23 “(2) The description under paragraph (1) shall be
24 based on the risk assessments required under subsection

1 (b)(2)(1) and operational evaluations required under sec-
2 tion 3553(d).

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

8 **“§ 3557. Annual independent audit**

9 “(a) IN GENERAL.—(1) Each year each agency shall
10 have performed an independent audit of the information
11 security program and practices of that agency to deter-
12 mine the effectiveness of such program and practices.

13 “(2) Each audit under this section shall include—

14 “(A) testing of the effectiveness of the informa-
15 tion systems of the agency for automated, contin-
16 uous monitoring of the state of compliance of its in-
17 formation systems with regulations promulgated
18 under section 3554 and standards promulgated
19 under section 3558 in a representative subset of—

20 “(i) the information systems used or oper-
21 ated by the agency; and

22 “(ii) the information systems used, oper-
23 ated, or supported on behalf of the agency by
24 a contractor of the agency, a subcontractor (at

1 any tier) of such contractor, or any other enti-
2 ty;

3 “(B) an assessment (made on the basis of the
4 results of the testing) of compliance with—

5 “(i) the requirements of this subchapter;
6 and

7 “(ii) related information security policies,
8 procedures, standards, and guidelines;

9 “(C) separate presentations, as appropriate, re-
10 garding information security relating to national se-
11 curity systems; and

12 “(D) a conclusion regarding whether the infor-
13 mation security controls of the agency are effective,
14 including an identification of any significant defi-
15 ciencies in such controls.

16 “(3) Each audit under this section shall be performed
17 in accordance with applicable generally accepted Govern-
18 ment auditing standards.

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

21 “(1) for each agency with an Inspector General
22 appointed under the Inspector General Act of 1978
23 or any other law, the annual audit required by this
24 section shall be performed by the Inspector General

1 or by an independent external auditor, as deter-
2 mined by the Inspector General of the agency; and

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

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

12 “(1) only by an entity designated head; and

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

18 “(d) EXISTING AUDITS.—The audit required by this
19 section may be based in whole or in part on another audit
20 relating to programs or practices of the applicable agency.

21 “(e) AGENCY REPORTING.—(1) Each year, not later
22 than such date established by the Director of the National
23 Office for Cyberspace, the head of each agency shall sub-
24 mit to the Director the results of the audit required under
25 this section.

1 “(2) To the extent an audit required under this sec-
2 tion directly relates to a national security system, the re-
3 sults of the audit submitted to the Director of the Na-
4 tional Office for Cyberspace shall contain only a summary
5 and assessment of that portion of the audit directly relat-
6 ing to a national security system.

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

13 “(g) OMB REPORTS TO CONGRESS.—(1) The Direc-
14 tor of the National Office for Cyberspace shall summarize
15 the results of the audits conducted under this section in
16 the annual report to Congress required under section
17 3555(a)(8).

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

1 “(3) Audits and any other descriptions of information
2 systems under the authority and control of the Director
3 of Central Intelligence or of National Foreign Intelligence
4 Programs systems under the authority and control of the
5 Secretary of Defense shall be made available to Congress
6 only through the appropriate oversight committees of Con-
7 gress, in accordance with applicable laws.

8 “(h) COMPTROLLER GENERAL.—The Comptroller
9 General shall periodically evaluate and report to Congress
10 on—

11 “(1) the adequacy and effectiveness of agency
12 information security policies and practices; and

13 “(2) implementation of the requirements of this
14 subchapter.

15 “(i) CONTRACTOR AUDITS.—Each year each con-
16 tractor that operates, uses, or supports an information
17 system by or on behalf of an agency and each subcon-
18 tractor of such contractor—

19 “(1) shall conduct an audit using an inde-
20 pendent external auditor, as determined by the
21 Comptroller General, in accordance with subsection
22 (a), including an assessment of compliance with the
23 applicable requirements of this subchapter; and

1 “(2) shall submit the results of such audit to
2 such agency not later than such date established by
3 the Agency.

4 **“§ 3558. Responsibilities for Federal information sys-**
5 **tems standards**

6 “(a) REQUIREMENT TO PRESCRIBE STANDARDS.—

7 “(1) IN GENERAL.—

8 “(A) REQUIREMENT.—Except as provided
9 under paragraph (2), the Director of the Office
10 of Management and Budget shall, on the basis
11 of proposed standards developed by the Na-
12 tional Institute of Standards and Technology
13 pursuant to paragraphs (2) and (3) of section
14 20(a) of the National Institute of Standards
15 and Technology Act (15 U.S.C. 278g-3(a)) and
16 in consultation with the Secretary of Homeland
17 Security, promulgate information security
18 standards pertaining to Federal information
19 systems.

20 “(B) REQUIRED STANDARDS.—Standards
21 promulgated under subparagraph (A) shall in-
22 clude—

23 “(i) standards that provide minimum
24 information security requirements as deter-
25 mined under section 20(b) of the National

1 Institute of Standards and Technology Act
2 (15 U.S.C. 278g-3(b)); and

3 “(ii) such standards that are other-
4 wise necessary to improve the efficiency of
5 operation or security of Federal informa-
6 tion systems.

7 “(C) REQUIRED STANDARDS BINDING.—
8 Information security standards described under
9 subparagraph (B) shall be compulsory and
10 binding.

11 “(2) STANDARDS AND GUIDELINES FOR NA-
12 TIONAL SECURITY SYSTEMS.—Standards and guide-
13 lines for national security systems, as defined under
14 section 3552(b), shall be developed, promulgated, en-
15 forced, and overseen as otherwise authorized by law
16 and as directed by the President.

17 “(b) APPLICATION OF MORE STRINGENT STAND-
18 ARDS.—The head of an agency may employ standards for
19 the cost-effective information security for all operations
20 and assets within or under the supervision of that agency
21 that are more stringent than the standards promulgated
22 by the Director of the Office of Management and Budget
23 under this section, if such standards—

1 “(1) contain, at a minimum, the provisions of
2 those applicable standards made compulsory and
3 binding by the Director; and

4 “(2) are otherwise consistent with policies and
5 guidelines issued under section 3555.

6 “(c) REQUIREMENTS REGARDING DECISIONS BY DI-
7 RECTOR.—

8 “(1) DEADLINE.—The decision regarding the
9 promulgation of any standard by the Director of the
10 Office of Management and Budget under subsection
11 (b) shall occur not later than 6 months after the
12 submission of the proposed standard to the Director
13 by the National Institute of Standards and Tech-
14 nology, as provided under section 20 of the National
15 Institute of Standards and Technology Act (15
16 U.S.C. 278g-3).

17 “(2) NOTICE AND COMMENT.—A decision by
18 the Director of the Office of Management and Budg-
19 et to significantly modify, or not promulgate, a pro-
20 posed standard submitted to the Director by the Na-
21 tional Institute of Standards and Technology, as
22 provided under section 20 of the National Institute
23 of Standards and Technology Act (15 U.S.C. 278g-
24 3), shall be made after the public is given an oppor-

1 tunity to comment on the Director’s proposed deci-
2 sion.

3 **“§ 3559. Federal information security incident center**

4 “(a) IN GENERAL.—The Director of the National Of-
5 fice for Cyberspace shall ensure the operation of a central
6 Federal information security incident center to—

7 “(1) provide timely technical assistance to oper-
8 ators of agency information systems regarding secu-
9 rity incidents, including guidance on detecting and
10 handling information security incidents;

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

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

16 “(4) consult with the National Institute of
17 Standards and Technology, agencies or offices oper-
18 ating or exercising control of national security sys-
19 tems (including the National Security Agency), and
20 such other agencies or offices in accordance with law
21 and as directed by the President regarding informa-
22 tion security incidents and related matters.

23 “(b) NATIONAL SECURITY SYSTEMS.—Each agency
24 operating or exercising control of a national security sys-
25 tem shall share information about information security in-

1 cidents, threats, and vulnerabilities with the Federal infor-
2 mation security incident center to the extent consistent
3 with standards and guidelines for national security sys-
4 tems, issued in accordance with law and as directed by
5 the President.

6 “(c) REVIEW AND APPROVAL.—In coordination with
7 the Administrator for Electronic Government and Infor-
8 mation Technology, the Director of the National Office for
9 Cyberspace shall review and approve the policies, proce-
10 dures, and guidance established in this subchapter to en-
11 sure that the incident center has the capability to effec-
12 tively and efficiently detect, correlate, respond to, contain,
13 and mitigate incidents that impair the adequate security
14 of the information systems and information infrastructure
15 of more than one agency. To the extent practicable, the
16 capability shall be continuous and technically automated.

17 **“§ 3560. National security systems**

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

21 “(1) provides information security protections
22 commensurate with the risk and magnitude of the
23 harm resulting from the unauthorized access, use,
24 disclosure, disruption, modification, or destruction of
25 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 **SEC. 3. INFORMATION SECURITY ACQUISITION REQUIRE-**
8 **MENTS.**

9 (a) IN GENERAL.—Chapter 113 of title 40, United
10 States Code, is amended by adding at the end of sub-
11 chapter II the following new section:

12 **“§ 11319. Information security acquisition require-**
13 **ments.**

14 “(a) PROHIBITION.—Notwithstanding any other pro-
15 vision of law, beginning one year after the date of the en-
16 actment of the Federal Information Security Amendments
17 Act of 2010, no agency may enter into a contract, an order
18 under a contract, or an interagency agreement for—

19 “(1) the collection, use, management, storage,
20 or dissemination of information on behalf of the
21 agency;

22 “(2) the use or operation of an information sys-
23 tem on behalf of the agency; or

24 “(3) information technology;

1 unless such contract, order, or agreement includes require-
2 ments to provide effective information security that sup-
3 ports the operations and assets under the control of the
4 agency, in compliance with the policies, standards, and
5 guidance developed under subsection (b), and otherwise
6 ensures compliance with this section.

7 “(b) COORDINATION OF SECURE ACQUISITION POLI-
8 CIES.—

9 “(1) IN GENERAL.—The Director, in consulta-
10 tion with the Director of the National Institute of
11 Standards and Technology, the Director of the Na-
12 tional Office for Cyberspace, and the Administrator
13 of General Services, shall oversee the development
14 and implementation of policies, standards, and guid-
15 ance, including through revisions to the Federal Ac-
16 quisition Regulation and the Department of Defense
17 supplement to the Federal Acquisition Regulation, to
18 cost effectively enhance agency information security,
19 including—

20 “(A) minimum information security re-
21 quirements for agency procurement of commer-
22 cial off-the-shelf information technology and
23 other products and services; and

24 “(B) approaches for evaluating and miti-
25 gating significant supply chain security risks

1 associated with products or services to be ac-
2 quired by agencies.

3 “(2) REPORT.—Not later than two years after
4 the date of the enactment of the Federal Informa-
5 tion Security Amendments Act of 2010, the Director
6 shall submit to Congress a report describing—

7 “(A) actions taken to improve the informa-
8 tion security associated with the procurement of
9 products and services by the Federal Govern-
10 ment; and

11 “(B) plans for overseeing and coordinating
12 efforts of agencies to use best practice ap-
13 proaches for cost-effectively purchasing more
14 secure products and services.

15 “(c) VULNERABILITY ASSESSMENTS OF MAJOR SYS-
16 TEMS.—

17 “(1) REQUIREMENT FOR INITIAL VULNER-
18 ABILITY ASSESSMENTS.—The Director shall require
19 each agency to conduct an initial vulnerability as-
20 sessment for any major system and its significant
21 items of supply prior to its development. The initial
22 vulnerability assessment of a major system and its
23 significant items of supply shall include use of an
24 analysis-based approach to—

25 “(A) identify vulnerabilities;

1 “(B) define exploitation potential;

2 “(C) examine the system’s potential effec-
3 tiveness;

4 “(D) determine overall vulnerability; and

5 “(E) make recommendations for risk re-
6 duction.

7 “(2) SUBSEQUENT VULNERABILITY ASSESS-
8 MENTS.—

9 “(A) The Director shall require, if the Di-
10 rector determines that a change in cir-
11 cumstances warrants the issuance of a subse-
12 quent vulnerability assessment, a subsequent
13 vulnerability assessment of each major system
14 and its significant items of supply within the
15 program.

16 “(B) Upon the request of a congressional
17 committee, the Director may require a subse-
18 quent vulnerability assessment of a particular
19 major system and its significant items of supply
20 within the program.

21 “(C) Any subsequent vulnerability assess-
22 ment of a major system and its significant
23 items of supply shall include use of an analysis-
24 based approach and, if applicable, a testing-
25 based approach, to monitor the exploitation po-

1 tential of such system and reexamine the fac-
2 tors described in subparagraphs (A) through
3 (E) of paragraph (1).

4 “(3) CONGRESSIONAL OVERSIGHT.—The Direc-
5 tor shall provide to the appropriate congressional
6 committees a copy of each vulnerability assessment
7 conducted under paragraph (1) or (2) not later than
8 10 days after the date of the completion of such as-
9 sessment.

10 “(d) DEFINITIONS.—In this section:

11 “(1) ITEM OF SUPPLY.—The term ‘item of sup-
12 ply’—

13 “(A) means any individual part, compo-
14 nent, subassembly, assembly, or subsystem inte-
15 gral to a major system, and other property
16 which may be replaced during the service life of
17 the major system, including a spare part or re-
18 plenishment part; and

19 “(B) does not include packaging or label-
20 ing associated with shipment or identification of
21 an item.

22 “(2) VULNERABILITY ASSESSMENT.—The term
23 ‘vulnerability assessment’ means the process of iden-
24 tifying and quantifying vulnerabilities in a major
25 system and its significant items of supply.

1 “(3) MAJOR SYSTEM.—The term ‘major system’
2 has the meaning given that term in section 4 of the
3 Office of Federal Procurement Policy Act (41 U.S.C.
4 403).”.

5 **SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.**

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

 “SUBCHAPTER II—INFORMATION SECURITY

- “3551. Purposes.
- “3552. Definitions.
- “3553. National Office for Cyberspace.
- “3554. Federal Cybersecurity Practice Board.
- “3555. Authority and functions of the Director of the National Office for
 Cyberspace.
- “3556. Agency responsibilities.
- “3557. Annual independent audit.
- “3558. Responsibilities for Federal information systems standards.
- “3559. Federal information security incident center.
- “3560. National security systems.”.

10 (b) TABLE OF SECTIONS IN TITLE 40.—The table
11 of sections for chapter 113 of title 40, United States Code,
12 is amended by inserting after the item relating to section
13 11318 the following new item:

 “Sec. 11319. Information security acquisition requirements.”.

14 (c) OTHER REFERENCES.—

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

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

4 (3) Section 2223(c)(3) of title 10, United
5 States Code, is amended, by striking “section
6 3542(b)(2))” and inserting “section 3552(b)”.

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

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

13 (A) in subsections (a)(2) and (e)(5), by
14 striking “section 3532(b)(2))” and inserting
15 “section 3552(b)”;

16 (B) in subsection (e)(2), by striking “sec-
17 tion 3532(1))” and inserting “section 3552(b)”;
18 and

19 (C) in subsections (c)(3) and (d)(1), by
20 striking “section 11331 of title 40” and insert-
21 ing “section 3558 of title 44”.

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 3556(b)”.

1 (d) REPEAL.—

2 (1) Subchapter III of chapter 113 of title 40,
3 United States Code, is repealed.

4 (2) The table of sections for chapter 113 of
5 such title is amended by striking the matter relating
6 to subchapter III.

7 **SEC. 5. EFFECTIVE DATE.**

8 This Act (including the amendments made by this
9 Act) shall take effect 30 days after the date of enactment
10 of this Act.

○