

112TH CONGRESS  
1ST SESSION

# H. R. 1136

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 16, 2011

Mr. LANGEVIN (for himself, Mr. BARTLETT, Mr. RUPPERSBERGER, Ms. LORETTA SANCHEZ of California, Mr. ANDREWS, and Mr. DICKS) introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## 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 “Executive Cyberspace Coordination Act of 2011”.

1 (b) TABLE OF CONTENTS.—The table of contents for  
 2 this Act is as follows:

Sec. 1. Short title.

TITLE I—FEDERAL INFORMATION SECURITY AMENDMENTS

Sec. 101. Coordination of Federal information policy.

Sec. 102. Information security acquisition requirements.

Sec. 103. Technical and conforming amendments.

Sec. 104. Effective date.

TITLE II—FEDERAL CHIEF TECHNOLOGY OFFICER

Sec. 201. Office of the Chief Technology Officer.

TITLE III—STRENGTHENING CYBERSECURITY FOR CRITICAL  
 INFRASTRUCTURE

Sec. 301. Definitions.

Sec. 302. Authority of Secretary.

3 **TITLE I—FEDERAL INFORMA-**  
 4 **TION SECURITY AMEND-**  
 5 **MENTS**

6 **SEC. 101. COORDINATION OF FEDERAL INFORMATION POL-**  
 7 **ICY.**

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

11 “SUBCHAPTER II—INFORMATION SECURITY  
 12 **“§ 3551. Purposes**

13 “The purposes of this subchapter are to—

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

1           “(2) recognize the highly networked nature of  
2           the current Federal computing environment and pro-  
3           vide effective Governmentwide management and  
4           oversight of the related information security risks,  
5           including coordination of information security efforts  
6           throughout the civilian, national security, and law  
7           enforcement communities;

8           “(3) provide for development and maintenance  
9           of minimum controls required to protect Federal in-  
10          formation and information infrastructure;

11          “(4) provide a mechanism for improved over-  
12          sight of Federal agency information security pro-  
13          grams;

14          “(5) acknowledge that commercially developed  
15          information security products offer advanced, dy-  
16          namic, robust, and effective information security so-  
17          lutions, reflecting market solutions for the protection  
18          of critical information infrastructures important to  
19          the national defense and economic security of the  
20          Nation that are designed, built, and operated by the  
21          private sector; and

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

1 **“§ 3552. Definitions**

2       “(a) SECTION 3502 DEFINITIONS.—Except as pro-  
3 vided under subsection (b), the definitions under section  
4 3502 shall apply to this subchapter.

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

6           “(1) The term ‘adequate security’ means secu-  
7 rity that complies with the regulations promulgated  
8 under section 3554 and the standards promulgated  
9 under section 3558.

10          “(2) The term ‘incident’ means an occurrence  
11 that actually or potentially jeopardizes the confiden-  
12 tiality, integrity, or availability of an information  
13 system, information infrastructure, or the informa-  
14 tion the system processes, stores, or transmits or  
15 that constitutes a violation or imminent threat of  
16 violation of security policies, security procedures, or  
17 acceptable use policies.

18          “(3) The term ‘information infrastructure’  
19 means the underlying framework that information  
20 systems and assets rely on in processing, storing, or  
21 transmitting information electronically.

22          “(4) The term ‘information security’ means  
23 protecting information and information infrastruc-  
24 ture from unauthorized access, use, disclosure, dis-  
25 ruption, modification, or destruction in order to pro-  
26 vide—

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

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

9           “(C) availability, which means ensuring  
10          timely and reliable access to and use of infor-  
11          mation; and

12          “(D) authentication, which means using  
13          digital credentials to assure the identity of  
14          users and validate access of such users.

15          “(5) The term ‘information technology’ has the  
16          meaning given that term in section 11101 of title  
17          40.

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

23                  “(i) the function, operation, or use of  
24                  which—

25                  “(I) involves intelligence activities;

1 “(II) involves cryptologic activities re-  
2 lated to national security;

3 “(III) involves command and control  
4 of military forces;

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

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

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

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

21 **“§ 3553. National Office for Cyberspace**

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

25 “(b) DIRECTOR.—

1           “(1) IN GENERAL.—There shall be at the head  
2 of the National Office for Cyberspace a Director,  
3 who shall be appointed by the President by and with  
4 the advice and consent of the Senate. The Director  
5 of the National Office for Cyberspace shall admin-  
6 ister all functions designated to such Director under  
7 this subchapter and collaborate to the extent prac-  
8 ticable with the heads of appropriate agencies, the  
9 private sector, and international partners. The Of-  
10 fice shall serve as the principal office for coordi-  
11 nating issues relating to cyberspace, including  
12 achieving an assured, reliable, secure, and survivable  
13 information infrastructure and related capabilities  
14 for the Federal Government, while promoting na-  
15 tional economic interests, security, and civil liberties.

16           “(2) BASIC PAY.—The Director of the National  
17 Office for Cyberspace shall be paid at the rate of  
18 basic pay for level III of the Executive Schedule.

19           “(c) STAFF.—The Director of the National Office for  
20 Cyberspace may appoint and fix the pay of additional per-  
21 sonnel as the Director considers appropriate.

22           “(d) EXPERTS AND CONSULTANTS.—The Director of  
23 the National Office for Cyberspace may procure temporary  
24 and intermittent services under section 3109(b) of title 5.

1 **“§ 3554. Federal Cybersecurity Practice Board**

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

6       “(b) MEMBERS.—The Board shall be chaired by the  
7 Director of the National Office for Cyberspace and consist  
8 of not more than 10 members, with at least one represent-  
9 ative from—

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

11               “(2) civilian agencies;

12               “(3) the Department of Defense;

13               “(4) the Federal law enforcement community;

14               “(5) the Federal Chief Technology Office; and

15               “(6) 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  
26 matters addressed in the policies and procedures are



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

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

7 “(A) MINIMUM SECURITY CONTROLS.—

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

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

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

20 “(B) MEASURES OF EFFECTIVENESS.—

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

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

5 “(C) PRODUCTS AND SERVICES.—The  
6 Board shall be responsible for developing and  
7 periodically updating information security poli-  
8 cies, procedures, and minimum security stand-  
9 ards relating to criteria for products and serv-  
10 ices to be used in agency information systems  
11 and information infrastructure that will meet  
12 the minimum security controls referred to in  
13 subparagraph (A). In carrying out this subpara-  
14 graph, the Board shall act in consultation with  
15 the Office of Management and Budget and the  
16 General Services Administration.

17 “(D) REMEDIES.—The Board shall be re-  
18 sponsible for developing and periodically updat-  
19 ing information security policies and procedures  
20 relating to methods for providing remedies for  
21 security deficiencies identified in agency infor-  
22 mation infrastructure.

23 “(3) ADDITIONAL CONSIDERATIONS.—The  
24 Board shall also consider—

1           “(A) opportunities to engage with the  
2 international community to set policies, prin-  
3 ciples, training, standards, or guidelines for in-  
4 formation security;

5           “(B) opportunities to work with agencies  
6 and industry partners to increase information  
7 sharing and policy coordination efforts in order  
8 to reduce vulnerabilities in the national infor-  
9 mation infrastructure; and

10           “(C) options necessary to encourage and  
11 maintain accountability of any agency, or senior  
12 agency official, for efforts to secure the infor-  
13 mation infrastructure of such agency.

14           “(4) RELATIONSHIP TO OTHER STANDARDS.—  
15 The policies and procedures developed under para-  
16 graph (1) are supplemental to the standards promul-  
17 gated by the Director of the National Office for  
18 Cyberspace under section 3558.

19           “(5) RECOMMENDATIONS FOR REGULATIONS.—  
20 The Board shall be responsible for making rec-  
21 ommendations to the Director of the National Office  
22 for Cyberspace on regulations to carry out the poli-  
23 cies and procedures developed by the Board under  
24 paragraph (1).

1 “(d) REGULATIONS.—The Director of the National  
2 Office for Cyberspace, in consultation with the Director  
3 of the Office of Management and the Administrator of  
4 General Services, shall promulgate and periodically update  
5 regulations to carry out the policies and procedures devel-  
6 oped by the Board under subsection (c).

7 “(e) ANNUAL REPORT.—The Director of the Na-  
8 tional Office for Cyberspace shall provide to Congress a  
9 report containing a summary of agency progress in imple-  
10 menting the regulations promulgated under this section as  
11 part of the annual report to Congress required under sec-  
12 tion 3555(a)(8).

13 “(f) NO DISCLOSURE BY BOARD REQUIRED.—The  
14 Board is not required to disclose under section 552 of title  
15 5 information submitted by agencies to the Board regard-  
16 ing threats, vulnerabilities, and risks.

17 **“§ 3555. Authority and functions of the Director of**  
18 **the National Office for Cyberspace**

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

22 “(1) developing and overseeing the implementa-  
23 tion of policies, principles, standards, and guidelines  
24 on information security, including through ensuring

1 timely agency adoption of and compliance with  
2 standards promulgated under section 3558;

3 “(2) requiring agencies, consistent with the  
4 standards promulgated under section 3558 and  
5 other requirements of this subchapter, to identify  
6 and provide information security protections com-  
7 mensurate with the risk and magnitude of the harm  
8 resulting from the unauthorized access, use, disclo-  
9 sure, disruption, modification, or destruction of—

10 “(A) information collected or maintained  
11 by or on behalf of an agency; or

12 “(B) information infrastructure used or  
13 operated by an agency or by a contractor of an  
14 agency or other organization on behalf of an  
15 agency;

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

1           “(4) overseeing agency compliance with the re-  
2 requirements of this subchapter, including through  
3 any authorized action under section 11303 of title  
4 40, to enforce accountability for compliance with  
5 such requirements;

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

9           “(6) coordinating information security policies  
10 and procedures of the Federal Government with re-  
11 lated information resources management policies and  
12 procedures on the security and resiliency of cyber-  
13 space;

14           “(7) overseeing the operation of the Federal in-  
15 formation security incident center required under  
16 section 3559;

17           “(8) reporting to Congress no later than March  
18 1 of each year on agency compliance with the re-  
19 quirements of this subchapter, including—

20                   “(A) a summary of the findings of audits  
21 required by section 3557;

22                   “(B) an assessment of the development,  
23 promulgation, and adoption of, and compliance  
24 with, standards developed under section 20 of  
25 the National Institute of Standards and Tech-

1 nology Act (15 U.S.C. 278g–3) and promul-  
2 gated under section 3558;

3 “(C) significant deficiencies in agency in-  
4 formation security practices;

5 “(D) planned remedial action to address  
6 such deficiencies; and

7 “(E) a summary of, and the views of the  
8 Director of the National Office for Cyberspace  
9 on, the report prepared by the National Insti-  
10 tute of Standards and Technology under section  
11 20(d)(10) of the National Institute of Stand-  
12 ards and Technology Act (15 U.S.C. 278g–3);

13 “(9) coordinating the defense of information in-  
14 frastructure operated by agencies in the case of a  
15 large-scale attack on information infrastructure, as  
16 determined by the Director;

17 “(10) establishing a national strategy not later  
18 than 120 days after the date of the enactment of  
19 this section;

20 “(11) coordinating information security training  
21 for Federal employees with the Office of Personnel  
22 Management;

23 “(12) ensuring the adequacy of protections for  
24 privacy and civil liberties in carrying out the respon-  
25 sibilities of the Director under this subchapter;

1           “(13) making recommendations that the Direc-  
2           tor determines are necessary to ensure risk-based se-  
3           curity of the Federal information infrastructure and  
4           information infrastructure that is owned, operated,  
5           controlled, or licensed for use by, or on behalf of, the  
6           Department of Defense, a military department, or  
7           another element of the intelligence community to—

8                   “(A) the Director of the Office of Manage-  
9                   ment and Budget;

10                   “(B) the head of an agency; or

11                   “(C) to Congress with regard to the re-  
12                   programming of funds;

13           “(14) ensuring, in consultation with the Admin-  
14           istrator of the Office of Information and Regulatory  
15           Affairs, that the efforts of agencies relating to the  
16           development of regulations, rules, requirements, or  
17           other actions applicable to the national information  
18           infrastructure are complementary;

19           “(15) when directed by the President, carrying  
20           out the responsibilities for national security and  
21           emergency preparedness communications described  
22           in section 706 of the Communications Act of 1934  
23           (47 U.S.C. 606) to ensure integration and coordina-  
24           tion; and



1           “(16) as assigned by the President, other duties  
2 relating to the security and resiliency of cyberspace.

3           “(b) RECRUITMENT PROGRAM.—Not later than 1  
4 year after appointment, the Director of the National Of-  
5 fice for Cyberspace shall establish a national program to  
6 conduct competitions and challenges that instruct United  
7 States students in cybersecurity education and computer  
8 literacy.

9           “(c) BUDGET OVERSIGHT AND REPORTING.—(1)  
10 The head of each agency shall submit to the Director of  
11 the National Office for Cyberspace a budget each year for  
12 the following fiscal year relating to the protection of infor-  
13 mation infrastructure for such agency, by a date deter-  
14 mined by the Director that is before the submission of  
15 such budget by the head of the agency to the Office of  
16 Management and Budget.

17           “(2) The Director shall review and offer a non-bind-  
18 ing approval or disapproval of each agency’s annual budg-  
19 et to each such agency before the submission of such budg-  
20 et by the head of the agency to the Office of Management  
21 and Budget.

22           “(3) If the Director offers a non-binding disapproval  
23 of an agency’s budget, the Director shall transmit rec-  
24 ommendations to the head of such agency for strength-

1 ening its proposed budget with regard to the protection  
2 of such agency's information infrastructure.

3 “(4) Each budget submitted by the head of an agency  
4 pursuant to paragraph (1) shall include—

5 “(A) a review of any threats to information  
6 technology for such agency;

7 “(B) a plan to secure the information infra-  
8 structure for such agency based on threats to infor-  
9 mation technology, using the National Institute of  
10 Standards and Technology guidelines and rec-  
11 ommendations;

12 “(C) a review of compliance by such agency  
13 with any previous year plan described in subpara-  
14 graph (B); and

15 “(D) a report on the development of the  
16 credentialing process to enable secure authentication  
17 of identity and authorization for access to the infor-  
18 mation infrastructure of such agency.

19 “(5) The Director of the National Office for Cyber-  
20 space may recommend to the President monetary penalties  
21 or incentives necessary to encourage and maintain ac-  
22 countability of any agency, or senior agency official, for  
23 efforts to secure the information infrastructure of such  
24 agency.

1 **“§ 3556. Agency responsibilities**

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

3 “(1) be responsible for—

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

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

11 “(ii) information infrastructure used  
12 or operated by an agency or by a con-  
13 tractor of an agency or other organization  
14 on behalf of an agency;

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

18 “(i) the regulations promulgated  
19 under section 3554 and the information se-  
20 curity standards promulgated under sec-  
21 tion 3558;

22 “(ii) information security standards  
23 and guidelines for national security sys-  
24 tems issued in accordance with law and as  
25 directed by the President; and

1           “(iii) ensuring the standards imple-  
2           mented for information infrastructure and  
3           national security systems under the agency  
4           head are complementary and uniform, to  
5           the extent practicable; and

6           “(C) ensuring that information security  
7           management processes are integrated with  
8           agency strategic and operational planning pro-  
9           cesses;

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

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

19               “(B) determining the levels of information  
20               security appropriate to protect such information  
21               and information infrastructure in accordance  
22               with regulations promulgated under section  
23               3554 and standards promulgated under section  
24               3558, for information security classifications  
25               and related requirements;

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

4           “(D) continuously testing and evaluating  
5           information security controls and techniques to  
6           ensure that they are effectively implemented;

7           “(3) delegate to an agency official, designated  
8           as the ‘Chief Information Security Officer’, under  
9           the authority of the agency Chief Information Offi-  
10          cer the responsibility to oversee agency information  
11          security and the authority to ensure and enforce  
12          compliance with the requirements imposed on the  
13          agency under this subchapter, including—

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

18                         “(i) assess the state of compliance of  
19                         all networks and systems with prescribed  
20                         controls issued pursuant to section 3558  
21                         and report immediately any variance there-  
22                         from and, where appropriate and with the  
23                         approval of the agency Chief Information  
24                         Officer, shut down systems that are found  
25                         to be non-compliant;

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

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

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

1 Force, and the Inspector General of the  
2 agency;

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 Chief Information Security  
24 Officer, in coordination with other senior agency of-  
25 ficials, reports biannually to the agency head on the

1 effectiveness of the agency information security pro-  
2 gram, including progress of remedial actions; and

3 “(6) ensure that the Chief Information Security  
4 Officer possesses necessary qualifications, including  
5 education, professional certifications, training, expe-  
6 rience, and the security clearance required to admin-  
7 ister the functions described under this subchapter;  
8 and has information security duties as the primary  
9 duty of that official.

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

18 “(1) continuous automated technical monitoring  
19 of information infrastructure used or operated by an  
20 agency or by a contractor of an agency or other or-  
21 ganization on behalf of an agency to assure conform-  
22 ance with regulations promulgated under section  
23 3554 and standards promulgated under section  
24 3558;



1           “(2) testing of the effectiveness of security con-  
2           trols that are commensurate with risk (as defined by  
3           the National Institute of Standards and Technology  
4           and the National Office for Cyberspace) for agency  
5           information infrastructure;

6           “(3) policies and procedures that—

7                   “(A) mitigate and remediate, to the extent  
8                   practicable, information security vulnerabilities  
9                   based on the risk posed to the agency;

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

12                   “(C) ensure that information security is  
13                   addressed throughout the life cycle of each  
14                   agency information system and information in-  
15                   frastructure;

16                   “(D) ensure compliance with—

17                           “(i) the requirements of this sub-  
18                           chapter;

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

24                           “(iii) minimally acceptable system  
25                           configuration requirements, as determined

1 by the Director of the National Office for  
2 Cyberspace; and

3 “(iv) any other applicable require-  
4 ments, including—

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

9 “(II) the policy of the Director of  
10 the National Office for Cyberspace;

11 “(III) the National Institute of  
12 Standards and Technology guidance;  
13 and

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

17 “(E) develop, maintain, and oversee infor-  
18 mation security policies, procedures, and control  
19 techniques to address all applicable require-  
20 ments, including those issued under sections  
21 3555 and 3558; and

22 “(F) ensure the oversight and training of  
23 personnel with significant responsibilities for in-  
24 formation security with respect to such respon-  
25 sibilities;

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

6           “(5) to the extent practicable, automated and  
7 continuous technical monitoring for testing, and  
8 evaluation of the effectiveness and compliance of in-  
9 formation security policies, procedures, and prac-  
10 tices, including—

11                   “(A) management, operational, and tech-  
12 nical controls of every information infrastruc-  
13 ture identified in the inventory required under  
14 section 3505(b); and

15                   “(B) management, operational, and tech-  
16 nical controls relied on for an evaluation under  
17 section 3556;

18           “(6) a process for planning, implementing, eval-  
19 uating, and documenting remedial action to address  
20 any deficiencies in the information security policies,  
21 procedures, and practices of the agency;

22           “(7) to the extent practicable, continuous auto-  
23 mated technical monitoring for detecting, reporting,  
24 and responding to security incidents, consistent with

1 standards and guidelines issued by the Director of  
2 the National Office for Cyberspace, including—

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

5 “(B) notifying and consulting with the ap-  
6 propriate security operations response center;  
7 and

8 “(C) notifying and consulting with, as ap-  
9 propriate—

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

12 “(ii) the National Office for Cyber-  
13 space; and

14 “(iii) any other agency or office, in ac-  
15 cordance with law or as directed by the  
16 President; and

17 “(8) plans and procedures to ensure continuity  
18 of operations for information infrastructure that  
19 support the operations and assets of the agency.

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

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

1 “(A) the National Office for Cyberspace;

2 “(B) the Committee on Homeland Security  
3 and Governmental Affairs of the Senate;

4 “(C) the Committee on Oversight and Gov-  
5 ernment Reform of the House of Representa-  
6 tives;

7 “(D) other appropriate authorization and  
8 appropriations committees of Congress; and

9 “(E) the Comptroller General;

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

13 “(A) annual agency budgets;

14 “(B) information resources management of  
15 this subchapter;

16 “(C) information technology management  
17 under this chapter;

18 “(D) program performance under sections  
19 1105 and 1115 through 1119 of title 31, and  
20 sections 2801 and 2805 of title 39;

21 “(E) financial management under chapter  
22 9 of title 31, and the Chief Financial Officers  
23 Act of 1990 (31 U.S.C. 501 note; Public Law  
24 101–576) (and the amendments made by that  
25 Act);

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

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

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

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

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

16           “(d) PERFORMANCE PLAN.—(1) In addition to the  
17           requirements of subsection (c), each agency, in consulta-  
18           tion with the National Office for Cyberspace, shall include  
19           as part of the performance plan required under section  
20           1115 of title 31 a description of the resources, including  
21           budget, staffing, and training, that are necessary to imple-  
22           ment the program required under subsection (b).

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

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

6       “§ 3557. Annual independent audit

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

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

12               “(A) testing of the effectiveness of the informa-  
13 tion infrastructure of the agency for automated, con-  
14 tinuous monitoring of the state of compliance of its  
15 information infrastructure with regulations promul-  
16 gated under section 3554 and standards promul-  
17 gated under section 3558 in a representative subset  
18 of—

19                       “(i) the information infrastructure used or  
20 operated by the agency; and

21                       “(ii) the information infrastructure used,  
22 operated, or supported on behalf of the agency  
23 by a contractor of the agency, a subcontractor  
24 (at any tier) of such contractor, or any other  
25 entity;

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

3                   “(i) the requirements of this subchapter;

4           and

5                   “(ii) related information security policies,  
6 procedures, standards, and guidelines;

7           “(C) separate assessments, as appropriate, re-  
8 garding information security relating to national se-  
9 curity systems; and

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

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

17           “(b) INDEPENDENT AUDITOR.—Subject to sub-  
18 section (c)—

19                   “(1) for each agency with an Inspector General  
20 appointed under the Inspector General Act of 1978  
21 or any other law, the annual audit required by this  
22 section shall be performed by the Inspector General  
23 or by an independent external auditor, as deter-  
24 mined by the Inspector General of the agency; and



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

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

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

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

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

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

24           “(2) To the extent an audit required under this sec-  
25           tion directly relates to a national security system, the re-

1 sults of the audit submitted to the Director of the Na-  
2 tional Office for Cyberspace shall contain only a summary  
3 and assessment of that portion of the audit directly relat-  
4 ing to a national security system.

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

11 “(g) NATIONAL OFFICE FOR CYBERSPACE REPORTS  
12 TO CONGRESS.—(1) The Director of the National Office  
13 for Cyberspace shall summarize the results of the audits  
14 conducted under this section in the annual report to Con-  
15 gress required under section 3555(a)(8).

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

23 “(3) Audits and any other descriptions of information  
24 infrastructure under the authority and control of the Di-  
25 rector of Central Intelligence or of National Foreign Intel-

1 ligen­ce Programs systems under the authority and control  
2 of the Secretary of Defense shall be made available to Con-  
3 gress only through the appropriate oversight committees  
4 of Congress, in accordance with applicable laws.

5       “(h) COMPTROLLER GENERAL.—The Comptroller  
6 General shall periodically evaluate and report to Congress  
7 on—

8               “(1) the adequacy and effectiveness of agency  
9 information security policies and practices; and

10              “(2) implementation of the requirements of this  
11 subchapter.

12       “(i) CONTRACTOR AUDITS.—Each year each con-  
13 tractor that operates, uses, or supports an information  
14 system or information infrastructure on behalf of an agen-  
15 cy and each subcontractor of such contractor—

16              “(1) shall conduct an audit using an inde-  
17 pendent external auditor in accordance with sub-  
18 section (a), including an assessment of compliance  
19 with the applicable requirements of this subchapter;  
20 and

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

1 **“§ 3558. Responsibilities for Federal information sys-**  
2 **tems standards**

3 “(a) REQUIREMENT TO PRESCRIBE STANDARDS.—

4 “(1) IN GENERAL.—

5 “(A) REQUIREMENT.—Except as provided  
6 under paragraph (2), the Secretary of Com-  
7 merce shall, on the basis of proposed standards  
8 developed by the National Institute of Stand-  
9 ards and Technology pursuant to paragraphs  
10 (2) and (3) of section 20(a) of the National In-  
11 stitute of Standards and Technology Act (15  
12 U.S.C. 278g–3(a)) and in consultation with the  
13 Secretary of Homeland Security, promulgate in-  
14 formation security standards pertaining to Fed-  
15 eral information systems.

16 “(B) REQUIRED STANDARDS.—Standards  
17 promulgated under subparagraph (A) shall in-  
18 clude—

19 “(i) standards that provide minimum  
20 information security requirements as deter-  
21 mined under section 20(b) of the National  
22 Institute of Standards and Technology Act  
23 (15 U.S.C. 278g–3(b)); and

24 “(ii) such standards that are other-  
25 wise necessary to improve the efficiency of

1 operation or security of Federal informa-  
2 tion systems.

3 “(C) REQUIRED STANDARDS BINDING.—  
4 Information security standards described under  
5 subparagraph (B) shall be compulsory and  
6 binding.

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

13 “(b) APPLICATION OF MORE STRINGENT STAND-  
14 ARDS.—The head of an agency may employ standards for  
15 the cost-effective information security for all operations  
16 and assets within or under the supervision of that agency  
17 that are more stringent than the standards promulgated  
18 by the Secretary of Commerce under this section, if such  
19 standards—

20 “(1) contain, at a minimum, the provisions of  
21 those applicable standards made compulsory and  
22 binding by the Secretary; and

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

1       “(c) REQUIREMENTS REGARDING DECISIONS BY THE  
2 SECRETARY.—

3           “(1) DEADLINE.—The decision regarding the  
4 promulgation of any standard by the Secretary of  
5 Commerce under subsection (b) shall occur not later  
6 than 6 months after the submission of the proposed  
7 standard to the Secretary by the National Institute  
8 of Standards and Technology, as provided under sec-  
9 tion 20 of the National Institute of Standards and  
10 Technology Act (15 U.S.C. 278g–3).

11           “(2) NOTICE AND COMMENT.—A decision by  
12 the Secretary of Commerce to significantly modify,  
13 or not promulgate, a proposed standard submitted to  
14 the Secretary by the National Institute of Standards  
15 and Technology, as provided under section 20 of the  
16 National Institute of Standards and Technology Act  
17 (15 U.S.C. 278g–3), shall be made after the public  
18 is given an opportunity to comment on the Sec-  
19 retary’s proposed decision.

20 **“§ 3559. Federal information security incident center**

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

24           “(1) provide timely technical assistance to oper-  
25 ators of agency information systems and information

1 infrastructure regarding security incidents, including  
2 guidance on detecting and handling information se-  
3 curity incidents;

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

6 “(3) inform operators of agency information  
7 systems and information infrastructure about cur-  
8 rent and potential information security threats, and  
9 vulnerabilities; and

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

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

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

13 **“§ 3560. National security systems**

14       “The head of each agency operating or exercising  
15 control of a national security system shall be responsible  
16 for ensuring that the agency—

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

22               “(2) implements information security policies  
23 and practices as required by standards and guide-  
24 lines for national security systems, issued in accord-  
25 ance with law and as directed by the President; and



1           “(3) complies with the requirements of this sub-  
2 chapter.”.

3 **SEC. 102. INFORMATION SECURITY ACQUISITION REQUIRE-**  
4 **MENTS.**

5 Chapter 113 of title 40, United States Code, is  
6 amended by adding at the end of subchapter II the fol-  
7 lowing new section:

8 **“§ 11319. Information security acquisition require-**  
9 **ments.**

10       “(a) PROHIBITION.—Notwithstanding any other pro-  
11 vision of law, beginning one year after the date of the en-  
12 actment of the Executive Cyberspace Coordination Act of  
13 2011, no agency may enter into a contract, an order under  
14 a contract, or an interagency agreement for—

15           “(1) the collection, use, management, storage,  
16 or dissemination of information on behalf of the  
17 agency;

18           “(2) the use or operation of an information sys-  
19 tem or information infrastructure on behalf of the  
20 agency; or

21           “(3) information technology;  
22 unless such contract, order, or agreement includes require-  
23 ments to provide effective information security that sup-  
24 ports the operations and assets under the control of the  
25 agency, in compliance with the policies, standards, and

1 guidance developed under subsection (b), and otherwise  
2 ensures compliance with this section.

3 “(b) COORDINATION OF SECURE ACQUISITION POLI-  
4 CIES.—

5 “(1) IN GENERAL.—The Director of the Office  
6 of Management and Budget, in consultation with the  
7 Director of the National Institute of Standards and  
8 Technology, the Director of the National Office for  
9 Cyberspace, and the Administrator of General Serv-  
10 ices, shall oversee the development and implementa-  
11 tion of policies, standards, and guidance, including  
12 through revisions to the Federal Acquisition Regula-  
13 tion and the Department of Defense supplement to  
14 the Federal Acquisition Regulation, to cost effec-  
15 tively enhance agency information security, includ-  
16 ing—

17 “(A) minimum information security re-  
18 quirements for agency procurement of informa-  
19 tion technology products and services; and

20 “(B) approaches for evaluating and miti-  
21 gating significant supply chain security risks  
22 associated with products or services to be ac-  
23 quired by agencies.

24 “(2) REPORT.—Not later than two years after  
25 the date of the enactment of the Executive Cyber-

1 space Coordination Act of 2011, the Director of the  
2 Office of Management and Budget shall submit to  
3 Congress a report describing—

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

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

12 “(c) VULNERABILITY ASSESSMENTS OF MAJOR SYS-  
13 TEMS.—

14 “(1) REQUIREMENT FOR INITIAL VULNER-  
15 ABILITY ASSESSMENTS.—The Director of the Office  
16 of Management and Budget shall require each agen-  
17 cy to conduct an initial vulnerability assessment for  
18 any major system and its significant items of supply  
19 prior to the development of the system. The initial  
20 vulnerability assessment of a major system and its  
21 significant items of supply shall include use of an  
22 analysis-based approach to—

23 “(A) identify vulnerabilities;

24 “(B) define exploitation potential;

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

3           “(D) determine overall vulnerability; and

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

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

8           “(A) The Director shall require a subse-  
9           quent vulnerability assessment of each major  
10          system and its significant items of supply with-  
11          in a program if the Director determines that  
12          circumstances warrant the issuance of an addi-  
13          tional vulnerability assessment.

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

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

1           tors described in subparagraphs (A) through  
2           (E) of paragraph (1).

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

9           “(d) DEFINITIONS.—In this section:

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

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

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

21           “(2) VULNERABILITY ASSESSMENT.—The term  
22           ‘vulnerability assessment’ means the process of iden-  
23           tifying and quantifying vulnerabilities in a major  
24           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. 103. 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 (e) EXECUTIVE SCHEDULE PAY RATE.—Section  
8 5314 of title 5, United States Code, is amended by adding  
9 at the end the following:

10 “Director of the National Office for Cyber-  
11 space.”.

12 (f) MEMBERSHIP ON THE NATIONAL SECURITY  
13 COUNCIL.—Section 101(a) of the National Security Act  
14 of 1947 (50 U.S.C. 402(a)) is amended—

15 (1) by redesignating paragraphs (7) and (8) as  
16 paragraphs (8) and (9), respectively; and

17 (2) by inserting after paragraph (6) the fol-  
18 lowing:

19 “(7) the Director of the National Office for  
20 Cyberspace;”.

21 **SEC. 104. EFFECTIVE DATE.**

22 (a) IN GENERAL.—Unless otherwise specified in this  
23 section, this title (including the amendments made by this  
24 title) shall take effect 30 days after the date of enactment  
25 of this Act.



1 (b) NATIONAL OFFICE FOR CYBERSPACE.—Section  
2 3553 of title 44, United States Code, as added by section  
3 101 of this title, shall take effect 180 days after the date  
4 of enactment of this Act.

5 (c) FEDERAL CYBERSECURITY PRACTICE BOARD.—  
6 Section 3554 of title 44, United States Code, as added  
7 by section 101 of this title, shall take effect one year after  
8 the date of enactment of this Act.

9 **TITLE II—FEDERAL CHIEF**  
10 **TECHNOLOGY OFFICER**

11 **SEC. 201. OFFICE OF THE CHIEF TECHNOLOGY OFFICER.**

12 (a) ESTABLISHMENT AND STAFF.—

13 (1) ESTABLISHMENT.—

14 (A) IN GENERAL.—There is established in  
15 the Executive Office of the President an Office  
16 of the Federal Chief Technology Officer (in this  
17 section referred to as the “Office”).

18 (B) HEAD OF THE OFFICE.—

19 (i) FEDERAL CHIEF TECHNOLOGY OF-  
20 FICER.—The President shall appoint a  
21 Federal Chief Technology Officer (in this  
22 section referred to as the “Federal CTO”)  
23 who shall be the head of the Office.

1 (ii) COMPENSATION.—Section 5314 of  
2 title 5, United States Code, is amended by  
3 adding at the end the following:

4 “Federal Chief Technology Officer.”.

5 (2) STAFF OF THE OFFICE.—The President  
6 may appoint additional staff members to the Office.

7 (b) DUTIES OF THE OFFICE.—The functions of the  
8 Federal CTO are the following:

9 (1) Undertake fact-gathering, analysis, and as-  
10 sessment of the Federal Government’s information  
11 technology infrastructures, information technology  
12 strategy, and use of information technology, and  
13 provide advice on such matters to the President,  
14 heads of Federal departments and agencies, and  
15 government chief information officers and chief tech-  
16 nology officers.

17 (2) Lead an interagency effort, working with  
18 the chief technology and chief information officers of  
19 each of the Federal departments and agencies, to de-  
20 velop and implement a planning process to ensure  
21 that they use best-in-class technologies, share best  
22 practices, and improve the use of technology in sup-  
23 port of Federal Government requirements.

24 (3) Advise the President on information tech-  
25 nology considerations with regard to Federal budg-

1       ets and with regard to general coordination of the  
2       research and development programs of the Federal  
3       Government for information technology-related mat-  
4       ters.

5           (4) Promote technological innovation in the  
6       Federal Government, and encourage and oversee the  
7       adoption of robust cross-governmental architectures  
8       and standards-based information technologies, in  
9       support of effective operational and management  
10      policies, practices, and services across Federal de-  
11      partments and agencies and with the public and ex-  
12      ternal entities.

13          (5) Establish cooperative public-private sector  
14      partnership initiatives to achieve knowledge of tech-  
15      nologies available in the marketplace that can be  
16      used for improving governmental operations and in-  
17      formation technology research and development ac-  
18      tivities.

19          (6) Gather timely and authoritative information  
20      concerning significant developments and trends in  
21      information technology, and in national priorities,  
22      both current and prospective, and analyze and inter-  
23      pret the information for the purpose of determining  
24      whether the developments and trends are likely to

1 affect achievement of the priority goals of the Fed-  
2 eral Government.

3 (7) Develop, review, revise, and recommend cri-  
4 teria for determining information technology activi-  
5 ties warranting Federal support, and recommend  
6 Federal policies designed to advance the develop-  
7 ment and maintenance of effective and efficient in-  
8 formation technology capabilities, including human  
9 resources, at all levels of government, academia, and  
10 industry, and the effective application of the capa-  
11 bilities to national needs.

12 (8) Any other functions and activities that the  
13 President may assign to the Federal CTO.

14 (c) POLICY PLANNING; ANALYSIS AND ADVICE.—The  
15 Office shall serve as a source of analysis and advice for  
16 the President and heads of Federal departments and agen-  
17 cies with respect to major policies, plans, and programs  
18 of the Federal Government in accordance with the func-  
19 tions described in subsection (b).

20 (d) COORDINATION OF THE OFFICE WITH OTHER  
21 ENTITIES.—

22 (1) FEDERAL CTO ON DOMESTIC POLICY COUN-  
23 CIL.—The Federal CTO shall be a member of the  
24 Domestic Policy Council.

1           (2) FEDERAL CTO ON CYBER SECURITY PRAC-  
2           TICE BOARD.—The Federal CTO shall be a member  
3           of the Federal Cybersecurity Practice Board.

4           (3) OBTAIN INFORMATION FROM AGENCIES.—  
5           The Office may secure, directly from any depart-  
6           ment or agency of the United States, information  
7           necessary to enable the Federal CTO to carry out  
8           this section. On request of the Federal CTO, the  
9           head of the department or agency shall furnish the  
10          information to the Office, subject to any applicable  
11          limitations of Federal law.

12          (4) STAFF OF FEDERAL AGENCIES.—On re-  
13          quest of the Federal CTO, to assist the Office in  
14          carrying out the duties of the Office, the head of any  
15          Federal department or agency may detail personnel,  
16          services, or facilities of the department or agency to  
17          the Office.

18          (e) ANNUAL REPORT.—

19                (1) PUBLICATION AND CONTENTS.—The Fed-  
20                eral CTO shall publish, in the Federal Register and  
21                on a public Internet website of the Federal CTO, an  
22                annual report that includes the following:

23                    (A) Information on programs to promote  
24                    the development of technological innovations.

1 (B) Recommendations for the adoption of  
2 policies to encourage the generation of techno-  
3 logical innovations.

4 (C) Information on the activities and ac-  
5 complishments of the Office in the year covered  
6 by the report.

7 (2) SUBMISSION.—The Federal CTO shall sub-  
8 mit each report under paragraph (1) to—

9 (A) the President;

10 (B) the Committee on Oversight and Gov-  
11 ernment Reform of the House of Representa-  
12 tives;

13 (C) the Committee on Science and Tech-  
14 nology of the House of Representatives; and

15 (D) the Committee on Commerce, Science,  
16 and Transportation of the Senate.

17 **TITLE III—STRENGTHENING CY-**  
18 **BERSECURITY FOR CRITICAL**  
19 **INFRASTRUCTURE**

20 **SEC. 301. DEFINITIONS.**

21 In this title:

22 (1) CRITICAL INFORMATION INFRASTRUC-  
23 TURE.—The term “critical information infrastruc-  
24 ture” means the electronic information and commu-  
25 nications systems, software, and assets that control,

1 protect, process, transmit, receive, program, or store  
2 information in any form, including data, voice, and  
3 video, relied upon by critical infrastructure, indus-  
4 trial control systems such as supervisory control and  
5 data acquisition systems, and programmable logic  
6 controllers. This shall also include such systems of  
7 the Federal Government.

8 (2) SECRETARY.—The term “Secretary” means  
9 the Secretary of Homeland Security.

10 **SEC. 302. AUTHORITY OF SECRETARY.**

11 (a) IN GENERAL.—The Secretary shall have primary  
12 authority, in consultation with the Director of the Na-  
13 tional Office for Cyberspace and the Federal Cyberspace  
14 Practice Board, in the executive branch of the Federal  
15 Government in creation, verification, and enforcement of  
16 measures with respect to the protection of critical informa-  
17 tion infrastructure, including promulgating risk-informed  
18 information security practices and standards applicable to  
19 critical information infrastructures that are not owned by  
20 or under the direct control of the Federal Government.  
21 The Secretary should consult with appropriate private sec-  
22 tor entities, including private owners and operators of the  
23 affected infrastructure, to carry out this section.

1 (b) OTHER FEDERAL AGENCIES.—In establishing  
2 measures with respect to the protection of critical informa-  
3 tion infrastructure the Secretary shall—

4 (1) consult with the Secretary of Commerce, the  
5 Secretary of Defense, the National Institute of  
6 Standards and Technology, and other sector specific  
7 Federal regulatory agencies in exercising the author-  
8 ity referred to in subsection (a); and

9 (2) coordinate, through the Executive Office of  
10 the President, with sector specific Federal regulatory  
11 agencies, including the Federal Energy Regulatory  
12 Commission, in establishing enforcement mecha-  
13 nisms under the authority referred to in subsection  
14 (a).

15 (c) AUDITING AUTHORITY.—The Secretary may—

16 (1) conduct such audits as are necessary to en-  
17 sure that appropriate measures are taken to secure  
18 critical information infrastructure;

19 (2) issue such subpoenas as are necessary to  
20 determine compliance with Federal regulatory re-  
21 quirements for securing critical information infra-  
22 structure; and

23 (3) authorize sector specific Federal regulatory  
24 agencies to undertake such audits.

○