

111TH CONGRESS
1ST SESSION

S. 921

To amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 28, 2009

Mr. CARPER introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “United States Informa-
3 tion and Communications Enhancement Act of 2009” or
4 the “U.S. ICE Act of 2009”.

5 **SEC. 2. FINDINGS.**

6 The Congress finds the following:

7 (1) The development of an interconnected glob-
8 al information infrastructure has significantly en-
9 hanced the productivity, prosperity, and collabora-
10 tion of people, business, and governments worldwide.

11 (2) The information infrastructure of the
12 United States is a strategic national resource vital
13 to our democracy, economy, and security.

14 (3) The Federal Government must increasingly
15 rely on a trusted and resilient information infra-
16 structure to effectively and efficiently communicate
17 with and deliver services to citizens, enhance eco-
18 nomic prosperity, defend the Nation from attack,
19 and recover from natural disasters.

20 (4) Since 2002 the Federal Government has ex-
21 perience multiple high-profile breaches that re-
22 sulted in the theft of sensitive information amount-
23 ing to more than the entire print collection con-
24 tained in the Library of Congress, including person-
25 ally identifiable information, advanced scientific re-

1 search, and prenegotiated United States diplomatic
2 positions.

3 (5) On March 12, 2008 witnesses testified be-
4 fore a hearing held by the Subcommittee on Federal
5 Financial Management, Government Information,
6 Federal Services, and International Security of the
7 Committee on Homeland Security and Governmental
8 Affairs of the Senate that—

9 (A) implementation of the Federal Infor-
10 mation Security Management Act of 2002
11 (Public Law 107–296; 116 Stat. 2135) wastes
12 agency resources on paperwork exercise instead
13 of security;

14 (B) agencies do not fully understand what
15 information they hold, who has access to that
16 information, and whether the information has
17 been compromised; and

18 (C) agencies lack effective coordination for
19 mitigating and responding to cyber-related inci-
20 dents.

21 (6) The Federal Information Security Manage-
22 ment Act of 2002 (Public Law 107–296; 116 Stat.
23 2135) needs to be amended to increase the coordina-
24 tion of agency activities to enhance situational
25 awareness throughout the Federal Government using

1 more effective enterprise-wide automated moni-
2 toring, detection, and response capabilities.

3 **SEC. 3. COORDINATION OF FEDERAL INFORMATION POL-**
4 **ICY.**

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

8 “SUBCHAPTER II—INFORMATION SECURITY
9 “§ 3551. **Definitions**

10 “(a) Except as provided under subsection (b), the
11 definitions under section 3502 shall apply to this sub-
12 chapter.

13 “(b) In this subchapter:

14 “(1) The term ‘adequate security’ means secu-
15 rity commensurate with the risk and magnitude of
16 harm resulting from the loss, misuse, or unauthor-
17 ized access to, or modification, of information.

18 “(2) The term ‘Director’ means the Director of
19 the National Office for Cyberspace.

20 “(3) The term ‘incident’ means an occurrence
21 that actually or potentially jeopardizes the confiden-
22 tiality, integrity, or availability of an information
23 system or the information the system processes,
24 stores, or transmits or that constitutes a violation or

1 imminent threat of violation of security policies, se-
2 curity procedures, or acceptable use policies.

3 “(4) The term ‘information infrastructure’
4 means the underlying framework that information
5 systems and assets rely on in processing, transmit-
6 ting, receiving, or storing information electronically.

7 “(5) The term ‘information security’ means
8 protecting information and information systems
9 from unauthorized access, use, disclosure, disrupt-
10 tion, modification, or destruction in order to pro-
11 vide—

12 “(A) integrity, which means guarding
13 against improper information modification or
14 destruction, and includes ensuring information
15 nonrepudiation and authenticity;

16 “(B) confidentiality, which means pre-
17 serving authorized restrictions on access and
18 disclosure, including means for protecting per-
19 sonal privacy and proprietary information; and

20 “(C) availability, which means ensuring
21 timely and reliable access to and use of infor-
22 mation.

23 “(6) The term ‘information technology’ has the
24 meaning given that term in section 11101 of title
25 40.

1 “(7)(A) The term ‘national security system’
2 means any information system (including any tele-
3 communications system) used or operated by an
4 agency or by a contractor of an agency, or other or-
5 ganization on behalf of an agency—

6 “(i) the function, operation, or use of
7 which—

8 “(I) involves intelligence activities;

9 “(II) involves cryptologic activities re-
10 lated to national security;

11 “(III) involves command and control
12 of military forces;

13 “(IV) involves equipment that is an
14 integral part of a weapon or weapons sys-
15 tem; or

16 “(V) subject to subparagraph (B), is
17 critical to the direct fulfillment of military
18 or intelligence missions; or

19 “(ii) is protected at all times by procedures
20 established for information that have been spe-
21 cifically authorized under criteria established by
22 an Executive order or an Act of Congress to be
23 kept classified in the interest of national de-
24 fense or foreign policy.

1 “(1) enhances economic prosperity and facili-
2 tates market leadership for the United States infor-
3 mation and communications industry;

4 “(2) deters, prevents, detects, defends against,
5 responds to, and remediates interruptions and dam-
6 age to United States information and communica-
7 tions infrastructure;

8 “(3) ensures United States capabilities to oper-
9 ate in cyberspace in support of national goals; and

10 “(4) protects privacy rights and preserving civil
11 liberties of United States persons.

12 “(b) Notwithstanding any provision of law, regula-
13 tion, rule, or policy to the contrary, the National Office
14 for Cyberspace may—

15 “(1) direct the sponsorship of the security
16 clearances for Federal officers and employees (in-
17 cluding experts and consultants employed under sec-
18 tion 3109) whose responsibilities involve critical in-
19 frastructure in the interest of national security; and

20 “(2) employ experts and consultants under sec-
21 tion 3109 for cyber security-related work.

22 “(c) With respect to responsibilities with the Federal
23 Government, the National Office for Cyberspace shall—

24 “(1) provide recommendations to agencies on
25 measures that shall be required to be implemented

1 to mitigate vulnerabilities, attacks, and exploitations
2 discovered as a result of activities required pursuant
3 to this section;

4 “(2) oversee the implementation of policies,
5 principles, standards, and guidelines on information
6 security, including through ensuring timely agency
7 adoption of and compliance with standards promul-
8 gated under section 3556;

9 “(3) to the extent practicable—

10 “(A) prioritize the policies, principles,
11 standards, and guidelines developed under sec-
12 tion 3556 based upon the threat, vulnerability
13 and consequences of an information security in-
14 cident; and

15 “(B) develop guidance that requires agen-
16 cies to actively monitor the effective implemen-
17 tation of policies, principles, standards, and
18 guidelines developed under section 3556;

19 “(4) require agencies, consistent with the stand-
20 ards promulgated under such section 3556 and the
21 requirements of this subchapter, to identify and pro-
22 vide information security protections commensurate
23 with the risk and magnitude of the harm resulting
24 from the unauthorized access, use, disclosure, dis-
25 ruption, 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 “(5) coordinate and ensure that the develop-
7 ment of standards and guidelines under section 20
8 of the National Institute of Standards and Tech-
9 nology Act (15 U.S.C. 278g–3) and standards and
10 guidelines developed for national security systems
11 are, to the maximum extent practicable, complemen-
12 tary and unified;

13 “(6) oversee agency compliance with the re-
14 quirements of this subchapter, including coordi-
15 nating with the Office of Management and Budget
16 to use any authorized action under section 11303 of
17 title 40, to enforce accountability for compliance
18 with such requirements;

19 “(7) review at least annually, and approving or
20 disapproving, agency information security programs
21 required under section 3554(b); and

22 “(8) coordinate information security policies
23 and procedures with related information resources
24 management policies and procedures.

1 “(d)(1) After consultation with the appropriate agen-
2 cies, the Director shall oversee the effective implementa-
3 tion of governmentwide operational evaluations on a fre-
4 quent and recurring basis to evaluate whether agencies ef-
5 fectively—

6 “(A) monitor, detect, analyze, protect, report,
7 and respond against known vulnerabilities, attacks,
8 and exploitations;

9 “(B) report to and collaborate with the appro-
10 priate public and private security operation centers
11 and law enforcement agencies; and

12 “(C) mitigate the risk posed by previous suc-
13 cessful exploitations in a timely fashion and in order
14 to prevent future vulnerabilities, attacks, and exploi-
15 tations.

16 “(2) Not later than 30 days after receiving an oper-
17 ational evaluation under this subsection, the Director shall
18 ensure agencies evaluated under paragraph (1) develop a
19 plan for addressing recommendations and mitigating
20 vulnerabilities contained in the security reports identified
21 under paragraph (1), including a timeline and budget for
22 implementing such plan.

23 “(e) Not later than March 1 of each year, the Direc-
24 tor shall submit a report to Congress on the overall infor-

1 mation security posture of the communications and infor-
2 mation infrastructure of the United States, including—

3 “(1) the evaluations conducted under subsection
4 (d) for the United States Government;

5 “(2) a detailed assessment of the overall resil-
6 iency of the communications and information infra-
7 structure effectiveness of the United States and the
8 United States Government including the ability to
9 monitor, detect, mitigate, and respond to an inci-
10 dent;

11 “(3) a detailed assessment the information se-
12 curity effectiveness of each agency, including the
13 ability to monitor, detect, mitigate, collaborate, and
14 respond to an incident;

15 “(4) a detailed assessment of operational eval-
16 uations performed during the preceding fiscal year,
17 the results of such evaluations, and any actions that
18 remain to be taken under plans included in correc-
19 tive action reports under subsection (d);

20 “(5) a detailed assessment of the development,
21 promulgation, and adoption of, and compliance with,
22 standards developed under section 20 of the Na-
23 tional Institute of Standards and Technology Act
24 (15 U.S.C. 278g–3) and promulgated under section
25 3554, and recommendations for enhancement;

1 “(6) a detailed assessment of significant defi-
2 ciencies in the information security and reporting
3 practices of the Federal Government as applicable to
4 each agency;

5 “(7) planned remedial action to address defi-
6 ciencies described under paragraph (6), including an
7 associated budget and recommendations for relevant
8 executive and legislative branch actions;

9 “(8) a summary of the results of the inde-
10 pendent evaluations under section 3555; and

11 “(9) a detailed assessment of the effectiveness
12 of reporting to the National Cyber Investigative
13 Joint Task Force under section 3554.

14 “(f) Evaluations and any other descriptions of infor-
15 mation systems under the authority and control of the Di-
16 rector of National Intelligence or of National Foreign In-
17 telligence Programs systems under the authority and con-
18 trol of the Secretary of Defense shall be made available
19 to Congress only through the appropriate oversight com-
20 mittees of Congress, in accordance with applicable laws.

21 “(g)(1) In collaboration with the private sector and
22 in coordination with the Director of the Office of Manage-
23 ment and Budget, the National Institute of Standards and
24 Technology, and the General Service Administration, the
25 Director shall develop and implement policy, guidance,

1 and regulations that cost effectively enhance the security
2 of the Federal Government, including policy, guidance,
3 and regulations that—

4 “(A) to the extent practicable, standardize
5 security requirements (also known as ‘lock-
6 down configurations’) of commercial off-the-
7 shelf products and services (including cloud
8 products and services) purchased by the Fed-
9 eral Government;

10 “(B) to the extent practicable, obtain prod-
11 ucts and services with security configuration
12 baselines consistent with available security
13 standards and configurations and guidelines de-
14 veloped by the National Institute of Standards
15 and Technology;

16 “(C) incentivize agencies to purchase
17 standard products and services through the
18 General Service Administration in order to re-
19 duce the vulnerabilities and costs associated
20 with custom products and services; and

21 “(D) enable purchasing decisions to rea-
22 sonably and appropriately account for signifi-
23 cant supply chain security risks associated with
24 any particular product or service.

1 “(2) Not later than 180 days after the date of enact-
2 ment of the United States Information and Communica-
3 tions Enhancement Act of 2009, and annually thereafter,
4 the Director shall submit a report to Congress that in-
5 cludes—

6 “(A) a description of the cost savings and secu-
7 rity enhancements that can be achieved by using the
8 purchasing power of the Federal Government; and

9 “(B) recommendations for legislative or execu-
10 tive branch actions necessary to achieve such cost
11 savings.

12 **“§ 3554. Agency responsibilities**

13 “(a) The head of each agency shall—

14 “(1) be responsible for—

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

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

22 “(ii) information systems used or op-
23 erated by an agency or by a contractor of
24 an agency or other organization on behalf
25 of an agency;

1 “(B) complying with the requirements of
2 this subchapter and related policies, procedures,
3 standards, and guidelines, including—

4 “(i) information security standards
5 promulgated under section 3556;

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

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

15 “(C) ensuring that information security
16 management processes are integrated with
17 agency strategic and operational planning pro-
18 cesses;

19 “(2) ensure that senior agency officials provide
20 information security for the information and infor-
21 mation systems that support the operations and as-
22 sets under their control, including through—

23 “(A) assessing the risk and magnitude of
24 the harm that could result from the unauthor-
25 ized access, use, disclosure, disruption, modi-

1 fication, or destruction of such information or
2 information systems;

3 “(B) determining the levels of information
4 security appropriate to protect such information
5 and information systems in accordance with
6 standards promulgated under section 3556, for
7 information security classifications and related
8 requirements;

9 “(C) implementing policies and procedures
10 to cost effectively reduce risks to an acceptable
11 level; and

12 “(D) continuously testing and evaluating
13 information security controls and techniques to
14 ensure that they are effectively implemented;

15 “(3) delegate to an agency official designated as
16 the Chief Information Security Officer the authority
17 to ensure and enforce compliance with the require-
18 ments imposed on the agency under this subchapter,
19 including—

20 “(A) overseeing the establishment and
21 maintenance of a security operations capability
22 that on an automated and continuous basis
23 can—

24 “(i) detect, report, respond to, con-
25 tain, and mitigate incidents that impair

1 adequate security of the information and
2 information infrastructure, in accordance
3 with policy provided by the Director, in
4 consultation with the Chief Information
5 Officers Council, and guidance from the
6 National Institute of Standards and Tech-
7 nology;

8 “(ii) collaborate with the National Of-
9 fice for Cyberspace and appropriate public
10 and private sector security operations cen-
11 ters to address incidents that impact the
12 security of information and information in-
13 frastructure that extend beyond the control
14 of the agency; and

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

23 “(B) collaborating with the Administrator
24 for E-Government and the Chief Information
25 Officer to establish, maintain, and update an

1 enterprise network, system, storage, and secu-
2 rity architecture framework documentation to
3 be submitted quarterly to the National Office
4 for Cyberspace and the appropriate security op-
5 erations center, that includes—

6 “(i) documentation of how technical,
7 managerial, and operational security con-
8 trols are implemented throughout the
9 agency’s information infrastructure; and

10 “(ii) documentation of how the con-
11 trols described under subparagraph (A)
12 maintain the appropriate level of confiden-
13 tiality, integrity, and availability of infor-
14 mation and information systems based
15 on—

16 “(I) the policy of the Director;

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

20 “(III) the Chief Information Offi-
21 cers Council recommended ap-
22 proaches;

23 “(C) developing, maintaining, and over-
24 seeing an agency wide information security pro-
25 gram as required by subsection (b);

1 “(D) developing, maintaining, and over-
2 seeing information security policies, procedures,
3 and control techniques to address all applicable
4 requirements, including those issued under sec-
5 tions 3553 and 3556;

6 “(E) training and overseeing personnel
7 with significant responsibilities for information
8 security with respect to such responsibilities;
9 and

10 “(F) assisting senior agency officials con-
11 cerning their responsibilities under paragraph
12 (2);

13 “(4) ensure that the agency has trained and
14 cleared personnel sufficient to assist the agency in
15 complying with the requirements of this subchapter
16 and related policies, procedures, standards, and
17 guidelines;

18 “(5) ensure that the agency Chief Information
19 Security Officer, in coordination with other senior
20 agency officials, reports biannually to the agency
21 head on the effectiveness of the agency information
22 security program, including progress of remedial ac-
23 tions; and

24 “(6) ensure that the Chief Information Security
25 Officer possesses necessary qualifications, including

1 education, professional certifications, training, expe-
2 rience, and the security clearance required to admin-
3 ister the functions described under this subchapter;
4 and has information security duties as the primary
5 duty of that official.

6 “(b) Each agency shall develop, document, and imple-
7 ment an agencywide information security program, ap-
8 proved by the Director under section 3553(a)(5), to pro-
9 vide information security for the information and informa-
10 tion systems that support the operations and assets of the
11 agency, including those provided or managed by another
12 agency, contractor, or other source, that includes—

13 “(1) periodic assessments—

14 “(A) of the risk and magnitude of the
15 harm that could result from the unauthorized
16 access, use, disclosure, disruption, modification,
17 or destruction of information and information
18 systems that support the operations and assets
19 of the agency; and

20 “(B) that recommend a prioritized descrip-
21 tion of which data and applications should be
22 removed or migrated to more secure networks
23 or standards;

24 “(2) penetration tests commensurate with risk
25 (as defined by the National Institute of Standards

1 and Technology and the National Office for Cyber-
2 space) for agency information systems;

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

5 “(4) policies and procedures that—

6 “(A) are based on the risk assessments re-
7 quired by paragraph (1);

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

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

13 “(D) 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, and infor-
18 mation security standards promulgated
19 under section 3556;

20 “(iii) minimally acceptable system
21 configuration requirements, as determined
22 by the Director; and

23 “(iv) any other applicable require-
24 ments, including standards and guidelines
25 for national security systems issued in ac-

1 cordance with law and as directed by the
2 President;

3 “(5) subordinate plans for providing adequate
4 information security for networks, facilities, and sys-
5 tems or groups of information systems, as appro-
6 priate;

7 “(6) role-based security awareness training to
8 inform personnel with access to the agency network,
9 including contractors and other users of information
10 systems that support the operations and assets of
11 the agency, of—

12 “(A) information security risks associated
13 with their activities; and

14 “(B) their responsibilities in complying
15 with agency policies and procedures designed to
16 reduce these risks;

17 “(7) to the extent practicable, automated and
18 continuous technical monitoring for testing, and
19 evaluation of the effectiveness and compliance of in-
20 formation security policies, procedures, and prac-
21 tices, including—

22 “(A) management, operational, and tech-
23 nical controls of every information system iden-
24 tified in the inventory required under section
25 3505(b); and

1 “(B) management, operational, and tech-
2 nical controls relied on for an evaluation under
3 section 3555;

4 “(8) a process for planning, implementing, eval-
5 uating, and documenting remedial action to address
6 any deficiencies in the information security policies,
7 procedures, and practices of the agency;

8 “(9) to the extent practicable, continuous tech-
9 nical monitoring for detecting, reporting, and re-
10 sponding to security incidents, consistent with stand-
11 ards and guidelines issued by the Director, includ-
12 ing—

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

15 “(B) notifying and consulting with the ap-
16 propriate security operations response center;
17 and

18 “(C) notifying and consulting with, as ap-
19 propriate—

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

22 “(ii) the National Office for Cyber-
23 space; and

1 “(iii) any other agency or office, in ac-
2 cordance with law or as directed by the
3 President; and

4 “(10) plans and procedures to ensure continuity
5 of operations for information systems that support
6 the operations and assets of the agency.

7 “(c) Each agency shall—

8 “(1) submit an annual report on the adequacy
9 and effectiveness of information security policies,
10 procedures, and practices, and compliance with the
11 requirements of this subchapter, including compli-
12 ance with each requirement of subsection (b) to—

13 “(A) the National Office for Cyberspace;

14 “(B) the Committee on Homeland Security
15 and Governmental Affairs of the Senate;

16 “(C) the Committee on Commerce,
17 Science, and Transportation of the Senate;

18 “(D) the Committee on Government Over-
19 sight and Reform of the House of Representa-
20 tives;

21 “(E) the Committee on Homeland Security
22 of the House of Representatives;

23 “(F) other appropriate authorization and
24 appropriations committees of Congress; and

25 “(G) the Comptroller General.

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

4 “(A) annual agency budgets;

5 “(B) information resources management of
6 this subchapter;

7 “(C) information technology management
8 under this chapter;

9 “(D) program performance under sections
10 1105 and 1115 through 1119 of title 31, and
11 sections 2801 and 2805 of title 39;

12 “(E) financial management under chapter
13 9 of title 31, and the Chief Financial Officers
14 Act of 1990 (31 U.S.C. 501 note; Public Law
15 101–576) (and the amendments made by that
16 Act);

17 “(F) financial management systems under
18 the Federal Financial Management Improve-
19 ment Act (31 U.S.C. 3512 note);

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

22 “(H) performance ratings, salaries, and
23 bonuses provided to the Chief Information Se-
24 curity Officer and supporting personnel taking
25 into account program performance; and

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

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

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

11 “(d)(1) In addition to the requirements of subsection
12 (c), each agency, in consultation with the National Office
13 for Cyberspace, shall include as part of the performance
14 plan required under section 1115 of title 31 a description
15 of—

16 “(A) the time periods; and

17 “(B) the resources, including budget, staffing,
18 and training, that are necessary to implement the
19 program required under subsection (b).

20 “(2) The description under paragraph (1) shall be
21 based on the risk assessments required under subsection
22 (b)(2)(1) and operational evaluations required under sec-
23 tion 3553(d).

24 “(e) Each agency shall provide the public with timely
25 notice and opportunities for comment on proposed infor-

1 mation security policies and procedures to the extent that
2 such policies and procedures affect communication with
3 the public.

4 **“§ 3555. Annual independent evaluation**

5 “(a)(1) Each year each agency shall have performed
6 an independent evaluation of the information security pro-
7 gram and practices of that agency to determine the effec-
8 tiveness of such program and practices.

9 “(2) Each evaluation under this section shall consist
10 of—

11 “(A) testing of the effectiveness of information
12 security policies, procedures, and practices of a rep-
13 resentative subset of the information systems of the
14 agency; and

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

17 “(i) the requirements of this subchapter;
18 and

19 “(ii) related information security policies,
20 procedures, standards, and guidelines.

21 “(b)(1) For each agency with an Inspector General
22 appointed under the Inspector General Act of 1978 (5
23 U.S.C. App.) or any other law, the annual evaluation re-
24 quired by this section shall be performed by the Inspector

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

3 “(2) For each agency to which paragraph (1) does
4 not apply, the head of the agency shall engage an inde-
5 pendent external auditor to perform the evaluation.

6 “(c) The evaluation required by this section may be
7 based in whole or in part on an audit, evaluation, or report
8 relating to programs or practices of the applicable agency.

9 “(d) Each year, not later than such date established
10 by the Director, the head of each agency shall submit to
11 the Director the results of the evaluation required under
12 this section.

13 “(e) Agencies and evaluators shall take appropriate
14 steps to ensure the protection of information which, if dis-
15 closed, may adversely affect information security. Such
16 protections shall be commensurate with the risk and com-
17 ply with all applicable laws and regulations.

18 “(f) The Comptroller General shall—

19 “(1) not later than 180 days after the date of
20 enactment of the United States Communications and
21 Information Enhancement Act of 2009 and after
22 collaboration with the Director and the Inspectors
23 General, develop and deliver standards for inde-
24 pendent evaluations as required under this section
25 that are risk-based and cost effective;

1 “(2) periodically evaluate and report to Con-
2 gress on—

3 “(A) the adequacy and effectiveness of
4 agency information security policies and prac-
5 tices; and

6 “(B) the implementation of the require-
7 ments of this subchapter.

8 **“§ 3556. Responsibilities for Federal information sys-**
9 **tems standards**

10 “(a)(1) The Secretary of Commerce shall, on the
11 basis of standards and guidelines developed by the Na-
12 tional Institute of Standards and Technology under para-
13 graphs (2) and (3) of section 20(a) of the National Insti-
14 tute of Standards and Technology Act (15 U.S.C. 278g–
15 3(a)), prescribe standards and guidelines pertaining to in-
16 formation systems, including national security systems.

17 “(2)(A) Standards prescribed under subsection (a)(1)
18 shall include information security standards that—

19 “(i) to the extent practicable, are unified with
20 standards and guidelines developed for information
21 systems and national security systems to ensure the
22 adequacy and effectiveness of information security
23 and information sharing;

24 “(ii) provide minimum information security re-
25 quirements as determined under section 20(b) of the

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

3 “(iii) are otherwise necessary to improve the se-
4 curity of information and information systems, in-
5 cluding information stored by third parties on behalf
6 of the Federal Government.

7 “(B) Information security standards described in
8 subparagraph (A) shall be compulsory and binding.

9 “(b) The President may disapprove or modify the
10 standards and guidelines referred to in subsection (a)(1)
11 if the President determines such action to be in the public
12 interest. The President’s authority to disapprove or mod-
13 ify such standards and guidelines may not be delegated.
14 Notice of such disapproval or modification shall be pub-
15 lished promptly in the Federal Register. Upon receiving
16 notice of such disapproval or modification, the Secretary
17 of Commerce shall immediately rescind or modify such
18 standards or guidelines as directed by the President.

19 “(c) To ensure fiscal and policy consistency, the Sec-
20 retary shall exercise the authority conferred by this section
21 subject to direction by the President and in coordination
22 with the Director of the Office of Management and Budget
23 and the National Office for Cyberspace.

24 “(d) The National Office for Cyberspace and the
25 head of an agency may employ standards for the cost ef-

1 fective information security for information systems within
2 or under the supervision of that agency that are more
3 stringent than the standards the Secretary prescribes
4 under this section if the more stringent standards—

5 “(1) contain at least the applicable standards
6 made compulsory and binding by the Secretary; and

7 “(2) are otherwise consistent with policies and
8 guidelines issued under section 3553.

9 “(e) The decision by the Secretary regarding the pro-
10 mulgation of any standard under this section shall occur
11 not later than 6 months after the submission of the pro-
12 posed standard to the Secretary by the National Institute
13 of Standards and Technology, as provided under section
14 20 of the National Institute of Standards and Technology
15 Act (15 U.S.C. 278g-3).”.

16 **SEC. 4. AUTHORITY AND RESPONSIBILITY OF THE UNITED**
17 **STATES COMPUTER EMERGENCY READINESS**
18 **TEAM IN RELATION TO FEDERAL AGENCIES.**

19 (a) DEFINITION.—In this section:

20 (1) The term “agency” has the meaning given
21 under section 3502(1) of title 44, United States
22 Code.

23 (2) The term “US-CERT” means the United
24 States Computer Emergency Readiness Team.

1 (b) PURPOSES.—The purposes of this section are to
2 recognize that US–CERT—

3 (1) is charged with providing response support
4 and defense against cyber attacks for agencies and
5 information sharing and collaboration with State
6 and local government, industry, and international
7 partners;

8 (2) interacts with agencies, industry, the re-
9 search community, State and local governments, and
10 others to disseminate reasoned and actionable cyber
11 security information to the public;

12 (3) provides a way for citizens, businesses, and
13 other institutions to communicate and coordinate di-
14 rectly with the United States Government about
15 cyber security; and

16 (4) has continually enhanced its ability to mon-
17 itor, detect, and respond to information security in-
18 cidents that affect the Federal Government.

19 (c) COORDINATION WITH US–CERT.—The head of
20 each agency shall ensure that the Chief Information Offi-
21 cer, Chief Information Security Officer, and security oper-
22 ations centers under the direction of that agency head
23 shall establish policies, procedures, and guidance to effec-
24 tively coordinate with the Director of US–CERT in a
25 timely fashion to detect, report, respond to, contain, and

1 mitigate incidents that impair adequate security of the in-
2 formation and information infrastructure.

3 (d) REVIEW AND APPROVAL.—In coordination with
4 the Administrator for Electronic Government and Infor-
5 mation Technology, the Director of the National Office for
6 Cyberspace shall review and approve the policies, proce-
7 dures, and guidance established in subparagraph (c) to en-
8 sure that US–CERT has the capability to effectively and
9 efficiently detect, correlate, respond to, contain, and miti-
10 gate incidents that impair the adequate security of the in-
11 formation and information infrastructure of more than 1
12 agency. To the extent practicable, the capability shall be
13 continuous and technically automated.

14 (e) SECURITY CLEARANCES; EXPERTS AND CON-
15 SULTANTS.—Notwithstanding any provision of law, regu-
16 lation, rule, or policy to the contrary, the Director of US–
17 CERT may—

18 (1) direct the sponsorship of the security clear-
19 ances for Federal officers and employees (including
20 experts and consultants employed under section
21 3109) whose responsibilities involve critical infra-
22 structure in the interest of national security; and

23 (2) employ experts and consultants under sec-
24 tion 3109 for cyber security-related work.

1 **SEC. 5. AUTHORITY AND RESPONSIBILITY OF DEPART-**
2 **MENTS NOT RELATED TO MILITARY FUNC-**
3 **TIONS.**

4 (a) DEFINITIONS.—In this section:

5 (1) AGENCY.—The term “agency”—

6 (A) means—

7 (i) an Executive department defined
8 under section 101 of title 5, United States
9 Code; and

10 (ii) an Executive agency that has mul-
11 tiple components which have separate and
12 distinct enterprise architectures; and

13 (B) shall not include—

14 (i) the Department of Defense; or

15 (ii) any component of an Executive
16 agency that is performing any national se-
17 curity function, including military intel-
18 ligence.

19 (2) EXECUTIVE AGENCY.—The term “Executive
20 agency” has the meaning given under section 105 of
21 title 5, United States Code.

22 (b) PURPOSE.—The purpose of this section is to rec-
23 ognize that—

24 (1) agencies have developed and maintained
25 separate and distinct enterprise architectures that
26 inhibit the ability of an agency to ensure that com-

1 ponents of that agency have effectively implemented
2 security policies, procedures, and practices;

3 (2) the separate and distinct enterprise archi-
4 tectures have in many instances been at the det-
5 riment of securing the agency information infra-
6 structure (the civilian cyberspace) and exposed that
7 infrastructure to unnecessary risk for an extended
8 period of time; and

9 (3) a more uniform agency enterprise architec-
10 ture will be more efficient and effective for the pur-
11 poses of information sharing and ensuring the ap-
12 propriate confidentiality, integrity, and availability of
13 information and information systems.

14 (c) AGENCY COORDINATION.—

15 (1) IN GENERAL.—Not later than 1 year after
16 the date of enactment of this Act, the head of each
17 agency shall ensure that components of that agency
18 shall establish an automated reporting mechanism
19 that allows the Chief Information Security Officer
20 and security operations center at the total agency
21 level to implement and monitor the implementation
22 of appropriate security policies, procedures, and con-
23 trols of agency components.

24 (2) APPROVAL AND COORDINATION.—The ac-
25 tivities conducted under paragraph (1) shall be—

1 (A) approved by the Director of the Na-
2 tional Office for Cyberspace; and

3 (B) to the extent practicable, in coordina-
4 tion and complementary with activities—

5 (i) described under section 4; and

6 (ii) conducted by the Administrator
7 for E-Government and Information Tech-
8 nology.

9 **SEC. 6. TECHNICAL AND CONFORMING AMENDMENTS.**

10 (a) **TABLE OF SECTIONS.**—The table of sections for
11 chapter 35 of title 44, United States Code, is amended
12 by striking the matter relating to subchapters II and III
13 and inserting the following:

“SUBCHAPTER II—INFORMATION SECURITY

“Sec. 3551. Definitions.

“Sec. 3552. National Office for Cyberspace.

“Sec. 3553. Authority and functions of the National Office for Cyberspace.

“Sec. 3554. Agency responsibilities.

“Sec. 3555. Annual independent evaluation.

“Sec. 3556. Responsibilities for Federal information systems standards.”.

14 (b) **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 3551(b)”.

19 (2) Section 2222(j)(6) of title 10, United States
20 Code, is amended by striking “section 3542(b)(2))”
21 and inserting “section 3551(b)”.

1 (3) Section 2223(c)(3) of title 10, United
2 States Code, is amended, by striking “section
3 3542(b)(2))” and inserting “section 3551(b)”.

4 (4) Section 2315 of title 10, United States
5 Code, is amended by striking “section 3542(b)(2))”
6 and inserting “section 3551(b)”.

7 (5) Section 20(a)(2) of the National Institute of
8 Standards and Technology Act (15 U.S.C. 278g–3)
9 is amended by striking “section 3532(b)(2)” and in-
10 sserting “section 3551(b)”.

11 (6) Section 8(d)(1) of the Cyber Security Re-
12 search and Development Act (15 U.S.C. 7406(d)(1))
13 is amended by striking “section 3534(b)” and in-
14 sserting “section 3554(b)”.

15 **SEC. 7. EFFECTIVE DATE.**

16 This Act (including the amendments made by this
17 Act) shall take effect 30 days after the date of enactment
18 of this Act.

○