

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 4257
OFFERED BY MR. ISSA OF CALIFORNIA**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Federal Information
3 Security Amendments Act of 2012”.

**4 SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-
5 ICY.**

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

9 “SUBCHAPTER II—INFORMATION SECURITY

10 “§ 3551. Purposes

11 “The purposes of this subchapter are to—

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

16 “(2) recognize the highly networked nature of
17 the current Federal computing environment and pro-
18 vide effective Governmentwide management and

1 oversight of the related information security risks,
2 including coordination of information security efforts
3 throughout the civilian, national security, and law
4 enforcement communities assets;

5 “(3) provide for development and maintenance
6 of minimum controls required to protect Federal in-
7 formation and information systems;

8 “(4) provide a mechanism for improved over-
9 sight of Federal agency information security pro-
10 grams and systems through a focus on automated
11 and continuous monitoring of agency information
12 systems and regular threat assessments;

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

21 “(6) recognize that the selection of specific
22 technical hardware and software information secu-
23 rity solutions should be left to individual agencies
24 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) ADEQUATE SECURITY.—The term ‘ade-
7 quate security’ means security commensurate with
8 the risk and magnitude of the harm resulting from
9 the unauthorized access to or loss, misuse, destruc-
10 tion, or modification of information.

11 “(2) AUTOMATED AND CONTINUOUS MONI-
12 TORING.—The term ‘automated and continuous
13 monitoring’ means monitoring, with minimal human
14 involvement, through an uninterrupted, ongoing real
15 time, or near real-time process used to determine if
16 the complete set of planned, required, and deployed
17 security controls within an information system con-
18 tinue to be effective over time with rapidly changing
19 information technology and threat development.

20 “(3) INCIDENT.—The term ‘incident’ means an
21 occurrence that actually or potentially jeopardizes
22 the confidentiality, integrity, or availability of an in-
23 formation system, or the information the system
24 processes, stores, or transmits or that constitutes a
25 violation or imminent threat of violation of security

1 policies, security procedures, or acceptable use poli-
2 cies.

3 “(4) INFORMATION SECURITY.—The term ‘in-
4 formation security’ means protecting information
5 and information systems from unauthorized access,
6 use, disclosure, disruption, modification, or destruc-
7 tion in order to provide—

8 “(A) integrity, which means guarding
9 against improper information modification or
10 destruction, and includes ensuring information
11 nonrepudiation and authenticity;

12 “(B) confidentiality, which means pre-
13 serving authorized restrictions on access and
14 disclosure, including means for protecting per-
15 sonal privacy and proprietary information; and

16 “(C) availability, which means ensuring
17 timely and reliable access to and use of infor-
18 mation.

19 “(5) INFORMATION SYSTEM.—The term ‘infor-
20 mation system’ means a discrete set of information
21 resources organized for the collection, processing,
22 maintenance, use, sharing, dissemination, or disposi-
23 tion of information and includes—

24 “(A) computers and computer networks;

25 “(B) ancillary equipment;

1 “(C) software, firmware, and related proce-
2 dures;

3 “(D) services, including support services;
4 and

5 “(E) related resources.

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

9 “(7) NATIONAL SECURITY SYSTEM.—

10 “(A) DEFINITION.—The term ‘national se-
11 curity system’ means any information system
12 (including any telecommunications system) used
13 or operated by an agency or by a contractor of
14 an agency, or other organization on behalf of an
15 agency—

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

18 “(I) involves intelligence activi-
19 ties;

20 “(II) involves cryptologic activi-
21 ties related to national security;

22 “(III) involves command and
23 control of military forces;

1 “(IV) involves equipment that is
2 an integral part of a weapon or weap-
3 ons system; or

4 “(V) subject to subparagraph
5 (B), is critical to the direct fulfillment
6 of military or intelligence missions; or

7 “(ii) is protected at all times by proce-
8 dures established for information that have
9 been specifically authorized under criteria
10 established by an Executive order or an
11 Act of Congress to be kept classified in the
12 interest of national defense or foreign pol-
13 icy.

14 “(B) EXCEPTION.—Subparagraph
15 (A)(i)(V) does not include a system that is to
16 be used for routine administrative and business
17 applications (including payroll, finance, logis-
18 tics, and personnel management applications).

19 “(8) THREAT ASSESSMENT.—The term ‘threat
20 assessment’ means the formal description and eval-
21 uation of threat to an information system.

22 **“§ 3553. Authority and functions of the Director**

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

1 “(1) developing and overseeing the implementa-
2 tion of policies, principles, standards, and guidelines
3 on information security, including through ensuring
4 timely agency adoption of and compliance with
5 standards promulgated under section 11331 of title
6 40;

7 “(2) requiring agencies, consistent with the
8 standards promulgated under such section 11331
9 and the requirements of this subchapter, to identify
10 and provide information security protections com-
11 mensurate with the risk and magnitude of the harm
12 resulting from the unauthorized access, use, disclo-
13 sure, disruption, modification, or destruction of—

14 “(A) information collected or maintained
15 by or on behalf of an agency; or

16 “(B) information systems used or operated
17 by an agency or by a contractor of an agency
18 or other organization on behalf of an agency;

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

1 guidelines are complementary with standards and
2 guidelines developed for national security systems;

3 “(4) overseeing agency compliance with the re-
4 quirements of this subchapter, including through
5 any authorized action under section 11303 of title
6 40, to enforce accountability for compliance with
7 such requirements;

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

11 “(6) coordinating information security policies
12 and procedures with related information resources
13 management policies and procedures;

14 “(7) overseeing the operation of the Federal in-
15 formation security incident center required under
16 section 3555; and

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) an assessment of the development,
21 promulgation, and adoption of, and compliance
22 with, standards developed under section 20 of
23 the National Institute of Standards and Tech-
24 nology Act (15 U.S.C. 278g-3) and promul-
25 gated under section 11331 of title 40;

1 “(B) significant deficiencies in agency in-
2 formation security practices;

3 “(C) planned remedial action to address
4 such deficiencies; and

5 “(D) a summary of, and the views of the
6 Director on, the report prepared by the Na-
7 tional Institute of Standards and Technology
8 under section 20(d)(10) of the National Insti-
9 tute of Standards and Technology Act (15
10 U.S.C. 278g-3).

11 “(b) NATIONAL SECURITY SYSTEMS.—Except for the
12 authorities described in paragraphs (4) and (8) of sub-
13 section (a), the authorities of the Director under this sec-
14 tion shall not apply to national security systems.

15 “(c) DEPARTMENT OF DEFENSE AND CENTRAL IN-
16 TELLIGENCE AGENCY SYSTEMS.—(1) The authorities of
17 the Director described in paragraphs (1) and (2) of sub-
18 section (a) shall be delegated to the Secretary of Defense
19 in the case of systems described in paragraph (2) and to
20 the Director of Central Intelligence in the case of systems
21 described in paragraph (3).

22 “(2) The systems described in this paragraph
23 are systems that are operated by the Department of
24 Defense, a contractor of the Department of Defense,
25 or another entity on behalf of the Department of

1 Defense that processes any information the unau-
2 thorized access, use, disclosure, disruption, modifica-
3 tion, or destruction of which would have a debili-
4 tating impact on the mission of the Department of
5 Defense.

6 “(3) The systems described in this paragraph
7 are systems that are operated by the Central Intel-
8 ligence Agency, a contractor of the Central Intel-
9 ligence Agency, or another entity on behalf of the
10 Central Intelligence Agency that processes any infor-
11 mation the unauthorized access, use, disclosure, dis-
12 ruption, modification, or destruction of which would
13 have a debilitating impact on the mission of the Cen-
14 tral Intelligence Agency.

15 **“§ 3554. Agency responsibilities**

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

17 “(1) be responsible for—

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

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

1 “(ii) information systems used or op-
2 erated by an agency or by a contractor of
3 an agency or other organization on behalf
4 of an agency;

5 “(B) complying with the requirements of
6 this subchapter and related policies, procedures,
7 standards, and guidelines, including—

8 “(i) information security standards
9 and guidelines promulgated under section
10 11331 of title 40 and section 20 of the Na-
11 tional Institute of Standards and Tech-
12 nology Act (15 U.S.C. 278g-3);

13 “(ii) information security standards
14 and guidelines for national security sys-
15 tems issued in accordance with law and as
16 directed by the President; and

17 “(iii) ensuring the standards imple-
18 mented for information systems and na-
19 tional security systems of the agency are
20 complementary and uniform, to the extent
21 practicable;

22 “(C) ensuring that information security
23 management processes are integrated with
24 agency strategic and operational planning and

1 budget processes, including policies, procedures,
2 and practices described in subsection (c)(2);

3 “(D) as appropriate, maintaining secure
4 facilities that have the capability of accessing,
5 sending, receiving, and storing classified infor-
6 mation;

7 “(E) maintaining a sufficient number of
8 personnel with security clearances, at the ap-
9 propriate levels, to access, send, receive and
10 analyze classified information to carry out the
11 responsibilities of this subchapter; and

12 “(F) ensuring that information security
13 performance indicators and measures are in-
14 cluded in the annual performance evaluations of
15 all managers, senior managers, senior executive
16 service personnel, and political appointees;

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

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

1 “(B) determining the levels of information
2 security appropriate to protect such information
3 and information systems in accordance with
4 policies, principles, standards, and guidelines
5 promulgated under section 11331 of title 40
6 and section 20 of the National Institute of
7 Standards and Technology Act (15 U.S.C.
8 278g–3) for information security classifications
9 and related requirements;

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

13 “(D) with a frequency sufficient to support
14 risk-based security decisions, testing and evalu-
15 ating information security controls and tech-
16 niques to ensure that such controls and tech-
17 niques are effectively implemented and oper-
18 ated; and

19 “(E) with a frequency sufficient to support
20 risk-based security decisions, conducting threat
21 assessments by monitoring information systems,
22 identifying potential system vulnerabilities, and
23 reporting security incidents in accordance with
24 paragraph (3)(A)(v);

1 “(3) delegate to the Chief Information Officer
2 or equivalent (or a senior agency official who reports
3 to the Chief Information Officer or equivalent), who
4 is designated as the ‘Chief Information Security Of-
5 ficer’, the authority and primary responsibility to de-
6 velop, implement, and oversee an agencywide infor-
7 mation security program to ensure and enforce com-
8 pliance with the requirements imposed on the agency
9 under this subchapter, including—

10 “(A) overseeing the establishment and
11 maintenance of a security operations capability
12 that through automated and continuous moni-
13 toring, when possible, can—

14 “(i) detect, report, respond to, con-
15 tain, and mitigate incidents that impair in-
16 formation security and agency information
17 systems, in accordance with policy provided
18 by the Director;

19 “(ii) commensurate with the risk to
20 information security, monitor and mitigate
21 the vulnerabilities of every information sys-
22 tem within the agency;

23 “(iii) continually evaluate risks posed
24 to information collected or maintained by
25 or on behalf of the agency and information

1 systems and hold senior agency officials
2 accountable for ensuring information secu-
3 rity;

4 “(iv) collaborate with the Director and
5 appropriate public and private sector secu-
6 rity operations centers to detect, report, re-
7 spond to, contain, and mitigate incidents
8 that impact the security of information
9 and information systems that extend be-
10 yond the control of the agency; and

11 “(v) report any incident described
12 under clauses (i) and (ii) to the Federal in-
13 formation security incident center, to other
14 appropriate security operations centers,
15 and to the Inspector General of the agen-
16 cy, to the extent practicable, within 24
17 hours after discovery of the incident, but
18 no later than 48 hours after such dis-
19 covery;

20 “(B) developing, maintaining, and over-
21 seeing an agencywide information security pro-
22 gram as required by subsection (b);

23 “(C) developing, maintaining, and over-
24 seeing information security policies, procedures,
25 and control techniques to address all applicable

1 requirements, including those issued under sec-
2 tion 11331 of title 40;

3 “(D) training and overseeing personnel
4 with significant responsibilities for information
5 security with respect to such responsibilities;
6 and

7 “(E) assisting senior agency officials con-
8 cerning their responsibilities under paragraph
9 (2);

10 “(4) ensure that the agency has a sufficient
11 number of trained and cleared personnel to assist
12 the agency in complying with the requirements of
13 this subchapter, other applicable laws, and related
14 policies, procedures, standards, and guidelines;

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

19 “(A) the effectiveness of the agency infor-
20 mation security program;

21 “(B) information derived from automated
22 and continuous monitoring, when possible, and
23 threat assessments; and

24 “(C) the progress of remedial actions;

1 “(6) ensure that the Chief Information Security
2 Officer possesses the necessary qualifications, includ-
3 ing education, training, experience, and the security
4 clearance required to administer the functions de-
5 scribed under this subchapter; and has information
6 security duties as the primary duty of that official;
7 and

8 “(7) ensure that components of that agency es-
9 tablish and maintain an automated reporting mecha-
10 nism that allows the Chief Information Security Of-
11 ficer with responsibility for the entire agency, and all
12 components thereof, to implement, monitor, and hold
13 senior agency officers accountable for the implemen-
14 tation of appropriate security policies, procedures,
15 and controls of agency components.

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

24 “(1) automated and continuous monitoring,
25 when possible, of the risk and magnitude of the

1 harm that could result from the disruption or unau-
2 thorized access, use, disclosure, modification, or de-
3 struction of information and information systems
4 that support the operations and assets of the agen-
5 cy;

6 “(2) consistent with guidance developed under
7 section 11331 of title 40, vulnerability assessments
8 and penetration tests commensurate with the risk
9 posed to agency information systems;

10 “(3) policies and procedures that—

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

13 “(B) 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 pursuant to section 11331 of title 40;

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

23 “(iv) any other applicable require-
24 ments, including—

1 “(I) standards and guidelines for
2 national security systems issued in ac-
3 cordance with law and as directed by
4 the President; and

5 “(II) the National Institute of
6 Standards and Technology standards
7 and guidance;

8 “(C) develop, maintain, and oversee infor-
9 mation security policies, procedures, and control
10 techniques to address all applicable require-
11 ments, including those promulgated pursuant
12 section 11331 of title 40; and

13 “(D) ensure the oversight and training of
14 personnel with significant responsibilities for in-
15 formation security with respect to such respon-
16 sibilities;

17 “(4) with a frequency sufficient to support risk-
18 based security decisions, automated and continuous
19 monitoring, when possible, for testing and evaluation
20 of the effectiveness and compliance of information
21 security policies, procedures, and practices, includ-
22 ing—

23 “(A) controls of every information system
24 identified in the inventory required under sec-
25 tion 3505(c); and

1 “(B) controls relied on for an evaluation
2 under this section;

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

7 “(6) with a frequency sufficient to support risk-
8 based security decisions, automated and continuous
9 monitoring, when possible, for detecting, reporting,
10 and responding to security incidents, consistent with
11 standards and guidelines issued by the National In-
12 stitute of Standards and Technology, including—

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

15 “(B) notifying and consulting with the
16 Federal information security incident center
17 and other appropriate security operations re-
18 sponse centers; and

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

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

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

1 “(7) plans and procedures to ensure continuity
2 of operations for information systems that support
3 the operations and assets of the agency.

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

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

10 “(A) the Director;

11 “(B) the Committee on Homeland Security
12 and Governmental Affairs of the Senate;

13 “(C) the Committee on Oversight and Gov-
14 ernment Reform of the House of Representa-
15 tives;

16 “(D) other appropriate authorization and
17 appropriations committees of Congress; and

18 “(E) the Comptroller General;

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

22 “(A) annual agency budgets;

23 “(B) information resources management of
24 this subchapter;

1 “(C) information technology management
2 under this chapter;

3 “(D) program performance under sections
4 1105 and 1115 through 1119 of title 31, and
5 sections 2801 and 2805 of title 39;

6 “(E) financial management under chapter
7 9 of title 31, and the Chief Financial Officers
8 Act of 1990 (31 U.S.C. 501 note; Public Law
9 101–576);

10 “(F) financial management systems under
11 the Federal Financial Management Improve-
12 ment Act of 1996 (31 U.S.C. 3512 note); and

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

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

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

20 “(B) if relating to financial management
21 systems, as an instance of a lack of substantial
22 compliance under the Federal Financial Man-
23 agement Improvement Act of 1996 (31 U.S.C.
24 3512 note).

1 **“§ 3555. Federal information security incident center**

2 “(a) IN GENERAL.—The Director shall ensure the
3 operation of a central Federal information security inci-
4 dent center to—

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

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

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

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

21 “(b) NATIONAL SECURITY SYSTEMS.—Each agency
22 operating or exercising control of a national security sys-
23 tem shall share information about information security in-
24 cidents, threats, and vulnerabilities with the Federal infor-
25 mation security incident center to the extent consistent
26 with standards and guidelines for national security sys-

1 tems, issued in accordance with law and as directed by
2 the President.

3 “(c) REVIEW AND APPROVAL.—The Director shall
4 review and approve the policies, procedures, and guidance
5 established in this subchapter to ensure that the incident
6 center has the capability to effectively and efficiently de-
7 tect, correlate, respond to, contain, mitigate, and reme-
8 diate incidents that impair the adequate security of the
9 information systems of more than one agency. To the ex-
10 tent practicable, the capability shall be continuous and
11 technically automated.

12 **“§ 3556. National security systems**

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

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

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

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

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

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

 “SUBCHAPTER II—INFORMATION SECURITY

 “3551. Purposes.

 “3552. Definitions.

 “3553. Authority and functions of the Director.

 “3554. Agency responsibilities.

 “3555. Federal information security incident center.

 “3556. National security systems.”.

8 (b) OTHER REFERENCES.—

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

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

16 (3) Section 2223(c)(3) of title 10, United
17 States Code, is amended, by striking “section
18 3542(b)(2))” and inserting “section 3552(b)”.

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

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

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

7 (B) in subsection (e)(2), by striking “sec-
8 tion 3532(1)” and inserting “section 3552(b)”.

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

13 **SEC. 4. EFFECTIVE DATE.**

14 This Act (including the amendments made by this
15 Act) shall take effect 30 days after the date of the enact-
16 ment of this Act.

