

ANNOUNCEMENT BY THE SPEAKER
PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on the motion to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote incurs objection under clause 6 of rule XX.

Any record vote on the postponed question will be taken later.

FEDERAL INFORMATION SECURITY
AMENDMENTS ACT OF 2012

Mr. ISSA. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4257) to amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes, as amended.

The Clerk read the title of the bill.
The text of the bill is as follows:

H.R. 4257

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

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

SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

“SUBCHAPTER II—INFORMATION
SECURITY

“§ 3551. Purposes

“The purposes of this subchapter are to—

“(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

“(2) recognize the highly networked nature of the current Federal computing environment and provide effective Governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities assets;

“(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

“(4) provide a mechanism for improved oversight of Federal agency information security programs and systems through a focus on automated and continuous monitoring of agency information systems and regular threat assessments;

“(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information systems important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and

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

“§ 3552. Definitions

“(a) SECTION 3502 DEFINITIONS.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

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

“(1) ADEQUATE SECURITY.—The term ‘adequate security’ means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

“(2) AUTOMATED AND CONTINUOUS MONITORING.—The term ‘automated and continuous monitoring’ means monitoring, with minimal human involvement, through an uninterrupted, ongoing real time, or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat development.

“(3) INCIDENT.—The term ‘incident’ means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

“(4) INFORMATION SECURITY.—The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

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

“(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

“(C) availability, which means ensuring timely and reliable access to and use of information.

“(5) INFORMATION SYSTEM.—The term ‘information system’ means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information and includes—

“(A) computers and computer networks;

“(B) ancillary equipment;

“(C) software, firmware, and related procedures;

“(D) services, including support services; and

“(E) related resources.

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

“(7) NATIONAL SECURITY SYSTEM.—

“(A) DEFINITION.—The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

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

“(I) involves intelligence activities;

“(II) involves cryptologic activities related to national security;

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

“(IV) involves equipment that is an integral part of a weapon or weapons system; or

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

“(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

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

“(8) THREAT ASSESSMENT.—The term ‘threat assessment’ means the formal description and evaluation of threat to an information system.

“§ 3553. Authority and functions of the Director

“(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

“(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

“(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

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

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

“(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

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

“(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3554(b);

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

“(7) overseeing the operation of the Federal information security incident center required under section 3555; and

“(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

“(A) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

“(B) significant deficiencies in agency information security practices;

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

“(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

“(b) NATIONAL SECURITY SYSTEMS.—Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.