require the Transportation Security Administration to implement best practices and improve transparency with regard to technology acquisition programs, and for other purposes, "aye;" rollcall vote No. 560—On Motion to Suspend the Rules and Concur in the Senate Amendment to H.R. 1204—To amend title 49, United States Code, to direct the Assistant Secretary of Homeland Security (Transportation Security Administration) to establish an Aviation Security Advisory Committee, and for other purposes, "aye."

NEWBORN SCREENING SAVES LIVES REAUTHORIZATION ACT OF 2014

Mrs. ELLMERS. Mr. Speaker, I ask unanimous consent to take from the Speaker's table the bill (H.R. 1281) to amend the Public Health Service Act to reauthorize programs under part A of title XI of such Act, with the Senate amendment thereto, and concur in the Senate amendment.

The Clerk read the title of the bill.

The SPEAKER pro tempore. The Clerk will report the Senate amendment.

The Clerk read as follows:

Senate amendment:

At the end, add the following:

SEC. 12. INFORMED CONSENT FOR NEWBORN SCREENING RESEARCH.

(a) IN GENERAL.—Research on newborn dried blood spots shall be considered research carried out on human subjects meeting the definition of section 46.102(f)(2) of title 45, Code of Federal Regulations, for purposes of Federally funded research conducted pursuant to the Public Health Service Act until such time as updates to the Federal Policy for the Protection of Human Subjects (the Common Rule) are promulgated pursuant to subsection (c). For purposes of this subsection, sections 46.116(c) and 46.116(d) of title 45, Code of Federal Regulations, shall not apply.

(b) EFFECTIVE DATE.—Subsection (a) shall apply only to newborn dried blood spots used for purposes of Federally funded research that were collected not earlier than 90 days after the date of enactment of this Act.

(c) REGULATIONS.—Not later than 6 months after the date of enactment of this Act, the Secretary of Health and Human Services shall promulgate proposed regulations related to the updating of the Federal Policy for the Protection of Human Subjects (the Common Rule), particularly with respect to informed consent. Not later than 2 years after such date of enactment, the Secretary shall promulgate final regulations based on such proposed regulations.

Mrs. ELLMERS (during the reading). Mr. Speaker, I ask unanimous consent that the reading of the Senate amendment be dispensed with.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from North Carolina?

There was no objection.

The SPEAKER pro tempore. Is there objection to the original request of the gentlewoman from North Carolina?

There was no objection.

A motion to reconsider was laid on the table.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

Mr. MEADOWS. Mr. Speaker, I ask unanimous consent to take from the Speaker's table the bill (S. 2521) to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security, and ask for its immediate consideration in the House.

The Clerk read the title of the bill.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from North Carolina?

There was no objection.

The text of the bill is as follows:

S. 2521

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 Modernization Act of 2014''.

SEC. 2. FISMA REFORM.

(a) IN GENERAL.—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;

''(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, including through automated security tools to continuously diagnose and improve security;

''(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 infrastructures 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) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

''(1) The term 'binding operational directive' means a compulsory direction to an agency that—

''(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

''(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

''(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

''(2) The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

''(3) 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.

''(4) The term 'information technology' has the meaning given that term in section 11101 of title 40.

''(5) The term 'intelligence community' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(6)(A) 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) 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).

''(7) The term 'Secretary' means the Secretary of Homeland Security.

''§ 3553. Authority and functions of the Director and the Secretary

''(a) DIRECTOR.—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