

Con. Res. 38, a concurrent resolution expressing the sense of Congress that Warren Weinstein should be returned home to his family.

S. RES. 578

At the request of Mr. MENENDEZ, the names of the Senator from New York (Mr. SCHUMER) and the Senator from Mississippi (Mr. COCHRAN) were added as cosponsors of S. Res. 578, a resolution supporting the role of the United States in ensuring children in the world's poorest countries have access to vaccines and immunization through Gavi, the Vaccine Alliance.

## SUBMITTED RESOLUTIONS

### SENATE RESOLUTION 595—RECOGNIZING NOBEL LAUREATES KAILASH SATYARTHI AND MALALA YOUSAFZAI FOR THEIR EFFORTS TO END THE FINANCIAL EXPLOITATION OF CHILDREN AND TO ENSURE THE RIGHT OF ALL CHILDREN TO AN EDUCATION

Mr. HARKIN submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 595

Whereas on October 10, 2014, the Norwegian Nobel Committee awarded the 2014 Nobel Peace Prize to Kailash Satyarthi and Malala Yousafzai;

Whereas the International Labour Organization estimates that, worldwide, 168,000,000 children are exploited financially, with 85,000,000 children working in very hazardous environments and deprived of an education;

Whereas the United Nations Educational, Scientific and Cultural Organization estimates that 121,000,000 children are not in school;

Whereas Kailash Satyarthi has personally rescued more than 82,000 children from the worst forms of child labor;

Whereas Malala Yousafzai has promoted education for girls in Pakistan since she was 11 years old and is an advocate for worldwide access to education;

Whereas Kailash Satyarthi has endured threats on his life as a result of such rescue efforts; and

Whereas the Taliban attempted to kill Malala Yousafzai on October 9, 2012, as a result of her efforts to encourage more girls to attend school: Now, therefore, be it

*Resolved*, That the Senate—

(1) recognizes Nobel Laureates Kailash Satyarthi and Malala Yousafzai as symbols of peace and advocates for ending the financial exploitation of children and for the right of all children to an education;

(2) commends all individuals working around the world to end the scourge of child slavery and to advance education for all children;

(3) recognizes the challenges that remain in ending the financial exploitation of children and providing access to an education for all children;

(4) urges all governments, civil society organizations, businesses, and individuals to unite in the common purpose of protecting children from losing their childhoods as well as their futures; and

(5) recognizes the dedication and commitment to freedom, the rights of children, and the endurance of the human spirit, demonstrated by all individuals who make sacrifices to build a more peaceful world.

## AMENDMENTS SUBMITTED AND PROPOSED

SA 3974. Mr. REID (for Mr. MENENDEZ) proposed an amendment to the bill S. 2142, to impose targeted sanctions on persons responsible for violations of human rights of antigovernment protesters in Venezuela, to strengthen civil society in Venezuela, and for other purposes.

SA 3975. Mr. REID (for Mr. CARPER (for himself and Mr. COBURN)) proposed an amendment to the bill S. 2521, to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

SA 3976. Mr. REID (for Mr. PAUL) proposed an amendment to the bill H.R. 1281, to amend the Public Health Service Act to reauthorize programs under part A of title XI of such Act.

## TEXT OF AMENDMENTS

**SA 3974.** Mr. REID (for Mr. MENENDEZ) proposed an amendment to the bill S. 2142, to impose targeted sanctions on persons responsible for violations of human rights of antigovernment protesters in Venezuela, to strengthen civil society in Venezuela, and for other purposes; as follows:

Strike all after the enacting clause and insert the following:

### SECTION 1. SHORT TITLE.

This Act may be cited as the “Venezuela Defense of Human Rights and Civil Society Act of 2014”.

### SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The Central Bank of Venezuela and the National Statistical Institute of Venezuela stated that the annual inflation rate in Venezuela in 2013 was 56.30, the highest level of inflation in the Western Hemisphere and the third highest level of inflation in the world behind South Sudan and Syria.

(2) The Central Bank of Venezuela and the Government of Venezuela have imposed a series of currency controls that has exacerbated economic problems and, according to the World Economic Forum, has become the most problematic factor for doing business in Venezuela.

(3) The Central Bank of Venezuela declared that the scarcity index of Venezuela reached 29.4 percent in March 2014, which signifies that fewer than one in 4 basic goods is unavailable at any given time. The Central Bank has not released any information on the scarcity index since that time.

(4) Since 1999, violent crime in Venezuela has risen sharply and the Venezuelan Violence Observatory, an independent nongovernmental organization, found the national per capita murder rate to be 79 per 100,000 people in 2013.

(5) The international nongovernmental organization Human Rights Watch recently stated, “Under the leadership of President Chávez and now President Maduro, the accumulation of power in the executive branch and the erosion of human rights guarantees have enabled the government to intimidate, censor, and prosecute its critics.”

(6) The Country Reports on Human Rights Practices for 2013 of the Department of State maintained that in Venezuela “the government did not respect judicial independence or permit judges to act according to the law without fear of retaliation” and “the government used the judiciary to intimidate and selectively prosecute political, union, business, and civil society leaders who were critical of government policies or actions”.

(7) The Government of Venezuela has detained foreign journalists and threatened and expelled international media outlets operating in Venezuela, and the international nongovernmental organization Freedom House declared that Venezuela’s “media climate is permeated by intimidation, sometimes including physical attacks, and strong antimedia rhetoric by the government is common”.

(8) Since February 4, 2014, the Government of Venezuela has responded to antigovernment protests with violence and killings perpetrated by its public security forces.

(9) In May 2014, Human Rights Watch found that the unlawful use of force perpetrated against antigovernment protesters was “part of a systematic practice by the Venezuelan security forces”.

(10) As of September 1, 2014, 41 people had been killed, approximately 3,000 had been arrested unjustly, and more than 150 remained in prison and faced criminal charges as a result of antigovernment demonstrations throughout Venezuela.

(11) Opposition leader Leopoldo Lopez was arrested on February 18, 2014, in relation to the protests and was unjustly charged with criminal incitement, conspiracy, arson, and property damage. Since his arrest, Lopez has been held in solitary confinement and has been denied 58 out of 60 of his proposed witnesses at his ongoing trial.

(12) As of September 1, 2014, not a single member of the public security forces of the Government of Venezuela had been held accountable for acts of violence perpetrated against antigovernment protesters.

### SEC. 3. SENSE OF CONGRESS REGARDING ANTIGOVERNMENT PROTESTS IN VENEZUELA AND THE NEED TO PREVENT FURTHER VIOLENCE IN VENEZUELA.

It is the sense of Congress that—

(1) the United States aspires to a mutually beneficial relationship with Venezuela based on respect for human rights and the rule of law and a functional and productive relationship on issues of public security, including counternarcotics and counterterrorism;

(2) the United States supports the people of Venezuela in their efforts to realize their full economic potential and to advance representative democracy, human rights, and the rule of law within their country;

(3) the chronic mismanagement by the Government of Venezuela of its economy has produced conditions of economic hardship and scarcity of basic goods and foodstuffs for the people of Venezuela;

(4) the failure of the Government of Venezuela to guarantee minimal standards of public security for its citizens has led the country to become one of the most violent and corrupt in the world;

(5) the Government of Venezuela continues to take steps to remove checks and balances on the executive, politicize the judiciary, undermine the independence of the legislature through use of executive decree powers, persecute and prosecute its political opponents, curtail freedom of the press, and limit the free expression of its citizens;

(6) Venezuelans, responding to ongoing economic hardship, high levels of crime and violence, and the lack of basic political rights and individual freedoms, have turned out in demonstrations in Caracas and throughout the country to protest the failure of the Government of Venezuela to protect the political and economic well-being of its citizens; and

(7) the repeated use of violence perpetrated by the National Guard and security personnel of Venezuela, as well as persons acting on behalf of the Government of Venezuela, against antigovernment protesters

that began on February 4, 2014, is intolerable and the use of unprovoked violence by protesters is also a matter of serious concern.

#### SEC. 4. UNITED STATES POLICY TOWARD VENEZUELA.

It is the policy of the United States—

(1) to support the people of Venezuela in their aspiration to live under conditions of peace and representative democracy as defined by the Inter-American Democratic Charter of the Organization of American States;

(2) to work in concert with the other member states within the Organization of American States, as well as the countries of the European Union, to ensure the peaceful resolution of the current situation in Venezuela and the immediate cessation of violence against antigovernment protestors;

(3) to hold accountable government and security officials in Venezuela responsible for or complicit in the use of force in relation to antigovernment protests and similar future acts of violence; and

(4) to continue to support the development of democratic political processes and independent civil society in Venezuela.

#### SEC. 5. SANCTIONS ON PERSONS RESPONSIBLE FOR VIOLENCE IN VENEZUELA.

(a) IN GENERAL.—The President shall impose the sanctions described in subsection (b) with respect to any foreign person, including any current or former official of the Government of Venezuela or any person acting on behalf of that Government, that the President determines—

(1) has perpetrated, or is responsible for ordering or otherwise directing, significant acts of violence or serious human rights abuses in Venezuela against persons associated with the antigovernment protests in Venezuela that began on February 4, 2014;

(2) has ordered or otherwise directed the arrest or prosecution of a person in Venezuela primarily because of the person's legitimate exercise of freedom of expression or assembly; or

(3) has knowingly materially assisted, sponsored, or provided significant financial, material, or technological support for, or goods or services in support of, the commission of acts described in paragraph (1) or (2).

(b) SANCTIONS DESCRIBED.—

(1) IN GENERAL.—The sanctions described in this subsection are the following:

(A) ASSET BLOCKING.—The exercise of all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person determined by the President to be subject to subsection (a) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(B) EXCLUSION FROM THE UNITED STATES AND REVOCATION OF VISA OR OTHER DOCUMENTATION.—In the case of an alien determined by the President to be subject to subsection (a), denial of a visa to, and exclusion from the United States of, the alien, and revocation in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)), of any visa or other documentation of the alien.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of paragraph (1)(A) or any regulation, license, or order issued to carry out paragraph (1)(A) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—The requirement to block and prohibit all transactions in all property and interests in property under paragraph (1)(A) shall not include the authority to impose sanctions on the importation of goods.

(4) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under paragraph (1)(B) shall not apply to an alien if admitting the alien into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(c) WAIVER.—The President may waive the application of sanctions under subsection (b) with respect to a person if the President—

(1) determines that such a waiver is in the national interest of the United States; and

(2) on or before the date on which the waiver takes effect, submits to the Committee on Foreign Relations and the Committee on Banking Housing, and Urban Affairs of the Senate and the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives a notice of and justification for the waiver.

(d) REGULATORY AUTHORITY.—The President shall issue such regulations, licenses, and orders as are necessary to carry out this section.

(e) TERMINATION.—The requirement to impose sanctions under this section shall terminate on December 31, 2016.

(f) DEFINITIONS.—In this section:

(1) ADMITTED; ALIEN.—The terms “admitted” and “alien” have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) FINANCIAL INSTITUTION.—The term “financial institution” has the meaning given that term in section 5312 of title 31, United States Code.

(3) FOREIGN PERSON.—The term “foreign person” means a person that is not a United States person.

(4) GOOD.—The term “good” has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. App. 2415) (as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)).

(5) KNOWINGLY.—The term “knowingly”, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(6) MATERIALLY ASSISTED.—The term “materially assisted” means the provision of assistance that is significant and of a kind directly relevant to acts described in paragraph (1) or (2) of subsection (a).

(7) UNITED STATES PERSON.—The term “United States person” means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

#### SEC. 6. REPORT ON BROADCASTING, INFORMATION DISTRIBUTION, AND CIRCUMVENTION TECHNOLOGY DISTRIBUTION IN VENEZUELA.

(a) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Chairman of the Broadcasting Board of Governors (in this section referred to as the “Board”) shall submit to Congress a report that includes—

(1) a thorough evaluation of the governmental, political, and technological obstacles faced by the people of Venezuela in their

efforts to obtain accurate, objective, and comprehensive news and information about domestic and international affairs;

(2) an assessment of current efforts relating to broadcasting, information distribution, and circumvention technology distribution in Venezuela, by the United States Government and otherwise; and

(3) a strategy for expanding such efforts in Venezuela, including recommendations for additional measures to expand upon current efforts.

(b) ELEMENTS.—The report required by subsection (a) shall include—

(1) an assessment of the current level of Federal funding dedicated to broadcasting, information distribution, and circumvention technology distribution in Venezuela by the Board before the date of the enactment of this Act;

(2) an assessment of the extent to which the current level and type of news and related programming and content provided by the Voice of America and other sources is addressing the informational needs of the people of Venezuela; and

(3) recommendations for increasing broadcasting, information distribution, and circumvention technology distribution in Venezuela.

**SA 3975.** Mr. REID (for Mr. CARPER (for himself and Mr. COBURN)) proposed an amendment to the bill S. 2521, to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security; as follows:

Strike all after the enacting clause and insert the following:

#### 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

“(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) ensuring that the Secretary carries out the authorities and functions under subsection (b);

“(4) 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;

“(5) 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; and

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

“(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

“(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

“(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

“(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

“(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

“(C) requirements for the mitigation of exogenous risks to information systems; and

“(D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

“(3) monitoring agency implementation of information security policies and practices;

“(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

“(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

“(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

“(A) operating the Federal information security incident center established under section 3556;

“(B) upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

“(C) compiling and analyzing data on agency information security; and

“(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems; and

“(7) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

“(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

“(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

“(2) a description of the threshold for reporting major information security incidents;

“(3) a summary of the results of evaluations required to be performed under section 3555;

“(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

“(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

“(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

“(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

“(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

“(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of

an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

“(f) CONSIDERATION.—

“(1) IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.

“(2) DIRECTIVES.—The Secretary shall—

“(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

“(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.

“(3) RULE OF CONSTRUCTION.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.

“(g) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

#### “§ 3554. Federal agency responsibilities

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

“(1) be responsible for—

“(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

“(i) information collected or maintained by or on behalf of the agency; and

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

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

“(i) information security standards promulgated under section 11331 of title 40;

“(ii) operational directives developed by the Secretary under section 3553(b);

“(iii) policies and procedures issued by the Director; and

“(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

“(C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;

“(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

“(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

“(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

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

“(D) periodically testing and evaluating information security controls and techniques

to ensure that they are effectively implemented;

“(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

“(A) designating a senior agency information security officer who shall—

“(i) carry out the Chief Information Officer's responsibilities under this section;

“(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

“(iii) have information security duties as that official's primary duty; and

“(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

“(B) developing and maintaining an agency-wide information security program as required by subsection (b);

“(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

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

“(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

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

“(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

“(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

“(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

“(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

“(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

“(2) policies and procedures that—

“(A) are based on the risk assessments required by paragraph (1);

“(B) cost-effectively reduce information security risks to an acceptable level;

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

“(D) ensure compliance with—

“(i) the requirements of this subchapter;

“(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

“(iii) minimally acceptable system configuration requirements, as determined by the agency; and

“(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

“(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

“(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

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

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

“(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

“(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);

“(B) may include testing relied on in an evaluation under section 3555; and

“(C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;

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

“(7) procedures for detecting, reporting, and responding to security incidents, which—

“(A) shall be consistent with the standards and guidelines described in section 3556(b);

“(B) may include using automated tools; and

“(C) shall include—

“(i) mitigating risks associated with such incidents before substantial damage is done;

“(ii) notifying and consulting with the Federal information security incident center established in section 3556; and

“(iii) notifying and consulting with, as appropriate—

“(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

“(II) an office designated by the President for any incident involving a national security system;

“(III) for a major incident, the committees of Congress described in subsection (c)(1)—

“(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

“(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

“(IV) any other agency or office, in accordance with law or as directed by the President; and

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

“(c) AGENCY REPORTING.—

“(1) ANNUAL REPORT.—

“(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

“(i) a description of each major information security incident or related sets of incidents, including summaries of—

“(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

“(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred;

“(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

“(IV) the detection, response, and remediation actions;

“(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

“(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

“(I) the number of individuals whose information was affected by the major information security incident; and

“(II) a description of the information that was breached or exposed; and

“(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

“(B) UNCLASSIFIED REPORT.—

“(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

“(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

“(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

“(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

“(A) the time periods; and

“(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

“(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

“(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

#### “§ 3555. Annual independent evaluation

“(a) IN GENERAL.—(1) Each year each agency shall have performed an independent eval-

uation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

“(2) Each evaluation under this section shall include—

“(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

“(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

“(C) separate presentations, as appropriate, regarding information security relating to national security systems.

“(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

“(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

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

“(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

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

“(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

“(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

“(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

“(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

“(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

“(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

“(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

“(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight com-

mittees of Congress, in accordance with applicable laws.

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

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

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

“(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

“(j) GUIDANCE.—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

#### “§ 3556. Federal information security incident center

“(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to—

“(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

“(2) compile and analyze information about incidents that threaten information security;

“(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;

“(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

“(5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

“(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

#### “§ 3557. National security systems

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

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

“(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

“(3) complies with the requirements of this subchapter.

**“§ 3558. Effect on existing law**

“Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.”.

(b) **MAJOR INCIDENT.**—The Director of the Office of Management and Budget shall—

(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.

(c) **CONTINUOUS DIAGNOSTICS.**—During the 2 year period beginning on the date of enactment of this Act, the Director of the Office of Management and Budget, with the assistance of the Secretary of Homeland Security, shall include in each report submitted under section 3553(c) of title 44, United States Code, as added by subsection (a), an assessment of the adoption by agencies of continuous diagnostics technologies, including through the Continuous Diagnostics and Mitigation program, and other advanced security tools to provide information security, including challenges to the adoption of such technologies or security tools.

(d) **BREACHES.**—

(1) **REQUIREMENTS.**—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall—

(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

(ii) include—

(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

(2) **NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.**—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

(3) **REPORTS.**—

(A) **DIRECTOR OF OMB.**—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis—

(i) assess agency implementation of data breach notification policies and guidelines in aggregate; and

(ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code.

(B) **SECRETARY OF HOMELAND SECURITY.**—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.

(4) **EXCEPTION.**—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

(5) **RULE OF CONSTRUCTION.**—Nothing in paragraph (1) shall be construed to alter any authority of a Federal agency or department.

(e) **TECHNICAL AND CONFORMING AMENDMENTS.**—

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

“SUBCHAPTER II—INFORMATION SECURITY

“3551. Purposes.

“3552. Definitions.

“3553. Authority and functions of the Director and the Secretary.

“3554. Federal agency responsibilities.

“3555. Annual independent evaluation.

“3556. Federal information security incident center.

“3557. National security systems.

“3558. Effect on existing law.”.

(2) **CYBERSECURITY RESEARCH AND DEVELOPMENT ACT.**—Section 8(d)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7406) is amended by striking “section 3534” and inserting “section 3554”.

(3) **HOMELAND SECURITY ACT OF 2002.**—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(A) in section 223 (6 U.S.C. 143)

(i) in the section heading, by inserting “**FEDERAL and**” before “**NON-FEDERAL**”;

(ii) in the matter preceding paragraph (1), by striking “the Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection” and inserting “the Under Secretary appointed under section 103(a)(1)(H)”;

(iii) in paragraph (2), by striking the period at the end and inserting “; and”;

(iv) by adding at the end the following:

“(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44, United States Code.”;

(B) in section 1001(c)(1)(A) (6 U.S.C. 511(c)(1)(A)), by striking “section 3532(3)” and inserting “section 3552(b)(5)”;

(C) in the table of contents in section 1(b), by striking the item relating to section 223 and inserting the following:

“Sec. 223. Enhancement of Federal and non-Federal cybersecurity.”.

(4) **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT.**—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) is amended—

(A) in subsection (a)(2), by striking “section 3532(b)(2)” and inserting “section 3552(b)(5)”;

(B) in subsection (e)—

(i) in paragraph (2), by striking “section 3532(1)” and inserting “section 3552(b)(2)”;

and

(ii) in paragraph (5), by striking “section 3532(b)(2)” and inserting “section 3552(b)(5)”.

(5) **TITLE 10.**—Title 10, United States Code, is amended—

(A) in section 2222(j)(5), by striking “section 3542(b)(2)” and inserting “section 3552(b)(5)”;

(B) in section 2223(c)(3), by striking “section 3542(b)(2)” and inserting “section 3552(b)(5)”;

(C) in section 2315, by striking “section 3542(b)(2)” and inserting “section 3552(b)(5)”.

(f) **OTHER PROVISIONS.**—

(1) **CIRCULAR A-130.**—Not later than 1 year after the date of enactment of this Act, the Director of the Office of Management and Budget shall amend or revise Office of Management and Budget Circular A-130 to eliminate inefficient or wasteful reporting. The Director of the Office of Management and Budget shall provide quarterly briefings to Congress on the status of the amendment or revision required under this paragraph.

(2) **ISPAB.**—Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4(b)) is amended—

(A) in paragraph (2), by inserting “, the Secretary of Homeland Security,” after “the Institute”;

(B) in paragraph (3), by inserting “the Secretary of Homeland Security,” after “the Secretary of Commerce.”.

**SA 3976.** Mr. REID (for Mr. PAUL) proposed an amendment to the bill H.R. 1281, to amend the Public Health Service Act to reauthorize programs under part A of title XI of such Act; as follows:

At the end, add the following:

**SEC. \_\_\_\_ 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.

#### AUTHORITY FOR COMMITTEES TO MEET

##### COMMITTEE ON VETERANS' AFFAIRS

Ms. KLOBUCHAR. Mr. President, I ask unanimous consent that the Committee on Veterans' Affairs be authorized to meet during the session of the Senate on December 8, 2014, at the time immediately following the first vote of the day, in room S-219 of the Capitol Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

#### PRIVILEGES OF THE FLOOR

Mr. LEE. Mr. President, I ask unanimous consent that privileges of the floor be granted to Neil Ashdown for the duration of 2014.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. HARKIN. Mr. President, I ask unanimous consent that Zachary Gross, Katy Crabtree, and Emalee Barto, interns with the Senate Health, Education, Labor, and Pensions Committee, be granted floor privileges for the remainder of today's session and that Caitlin Boon, a detailee with the committee, also be granted floor privileges for today's session.

The PRESIDING OFFICER. Without objection, it is so ordered.

#### FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

Mr. REID. I ask unanimous consent that the Senate proceed to the consideration of Calendar No. 564, S. 2521.

The PRESIDING OFFICER. The clerk will report the bill by title.

The bill clerk read as follows:

A bill (S. 2521) to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

There being no objection, the Senate proceeded to consider the bill.

Mr. REID. I ask unanimous consent that the Carper-Coburn substitute amendment, which is at the desk, be agreed to; the bill, as amended, be read a third time; and the Senate proceed to vote on passage.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment (No. 3975) in the nature of a substitute was agreed to.

(The amendment is printed in today's RECORD under "Text of Amendments.")

The bill was ordered to be engrossed for a third reading and was read the third time.

The PRESIDING OFFICER. Hearing no further debate, the bill having been read the third time, the question is, Shall it pass?

The bill (S. 2521), as amended, was passed.

Mr. REID. I ask unanimous consent that the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. REID. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. REID. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

#### APPOINTMENT

The PRESIDING OFFICER. The Chair announces, on behalf of the majority leader, pursuant to the provisions of Public Law 100-702, the appointment of the following individual to the board of the Federal Judicial Center Foundation: Peter Kraus of Texas.

Mr. REID. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. REID. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

#### NEWBORN SCREENING SAVES LIVES REAUTHORIZATION ACT OF 2014

Mr. REID. I ask unanimous consent that the Senate proceed to the consideration of H.R. 1281.

The PRESIDING OFFICER. The clerk will report the bill by title.

The bill clerk read as follows:

A bill (H.R. 1281) to amend the Public Health Service Act to reauthorize programs under part A of title XI of such Act.

There being no objection, the Senate proceeded to consider the bill.

Mr. REID. I ask unanimous consent that the Paul amendment, which is at the desk, be agreed to; the bill, as amended, be read a third time and passed; and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment (No. 3976) was agreed to, as follows:

(Purpose: To clarify rules relating to newborn screening research and informed consent)

At the end, add the following:

#### SEC. \_\_\_\_ 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 pursu-

ant 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.

The amendment was ordered to be engrossed, and the bill to be read a third time.

The bill was read the third time.

The bill (H.R. 1281), as amended, was passed.

#### MEASURES DISCHARGED

Mr. REID. I ask unanimous consent that the Homeland Security and Governmental Affairs Committee be discharged from further consideration of the following measures, which are post office-naming bills, and the Senate proceed to their consideration en bloc: H.R. 4939, H.R. 1707, H.R. 78, H.R. 2112, H.R. 2223, H.R. 2678, H.R. 3534, and H.R. 5030.

The PRESIDING OFFICER. Without objection, it is so ordered.

There being no objection, the Senate proceeded to consider the bills en bloc.

Mr. REID. I ask unanimous consent that the bills be read a third time and passed en bloc and the motions to reconsider be laid upon the table en bloc with no intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

#### NEIL HAVENS POST OFFICE

The bill (H.R. 4939) to designate the facility of the United States Postal Service located at 2551 Galena Avenue in Simi Valley, California, as the "Neil Havens Post Office," was ordered to a third reading, was read the third time, and passed.

#### JAMES R. BURGESS JR. POST OFFICE BUILDING

The bill (H.R. 1707) to designate the facility of the United States Postal Service located at 302 East Green Street in Champaign, Illinois, as the "James R. Burgess Jr. Post Office Building," was ordered to a third reading, was read the third time, and passed.

#### GEORGE THOMAS "MICKEY" LELAND POST OFFICE BUILDING

The bill (H.R. 78) to designate the facility of the United States Postal Service located at 4110 Alameda Road in