a significant depletion in their cash reserves and a freeze on capital expenditures. This circumstance is just not sustainable, and so we are seeing hospitals close.

Since about 1990, the number of rural hospitals across the country has remained stable at around 2,000, but last year 15 rural hospitals closed. We have to be concerned there are more to follow. This is an alarming trend. These hospitals play a vital role in health care to those rural communities. It can determine whether a community has a future—whether individuals and families will decide to live there. The loss of a hospital has huge ripple effects and it harms patients. Their primary purpose is to save lives and improve health care, but it is also a tremendous loss to the community itself.

I outlined problems that I believed would occur for hospitals with the passage of ObamaCare long before the law became law. I also would say it doesn't mean I don't believe there aren't significant improvements to be made to our health care delivery system, but I think the reality is that the Affordable Care Act causes more problems—significantly more problems—than those it solves.

Many Kansas hospitals struggle to meet the needs of the aging population in their States and the Affordable Care Act cuts are an exacerbation of their circumstance. Again, the Affordable Care Act had the promise of: If you like your plan, you can keep it. If you like your health insurance plan, you can keep it. If you like your physician, you can keep him or her. That didn't turn out to be true.

In fact, if you liked your policy, you were probably not able to keep it, and that something else now—that replacement policy—often involves increased copayments and deductibles. That certainly is a problem for the policyholder and his or her family. It is a problem for the business and their employees. But we may have forgotten it is a huge problem for the health care provider.

Almost every hospital I have visited, now that the Affordable Care Act is being implemented, will tell me about the increasing amount of unpaid hospital bills—the amount of money that is owed that is attempting to be recovered. The reason that occurs is because the copayments and deductibles are so significantly higher that patients don't have the ability to pay a $5,000 copayment or even a $1,000 copayment. So the hospital's bad debt is increasing because patients don't have the necessary amount of money to pay for their portion of what their health care insurance policy now requires of them.

Again, this comes from a law that was described to us as going to increase the affordability and the availability of health care. I guess what I would point out is, in the circumstance we are now in, the policies are so expensive, so much more costly both in premiums and copayments and deductibles, that the affordability is a problem again and not just for the patient, not for the policyholder but for the hospital that is now left holding the bag because so many of their patients can't pay the copayments or the deductibles.

When the Affordable Care Act passed, the President's own Medicare Chief Actuary noted that the cuts would cause as many as 15 percent of hospitals, skilled nursing facilities, and home health agencies to be unprofitable by 2019. While that point in time may have seemed a long time away, 2019 is now just about 5 years away. If ObamaCare remains in place, the estimated percentage of unprofitable providers is projected to increase, reaching roughly 25 percent in 2030 and 40 percent in 2050. So by 2030 25 percent of the hospitals, health care providers, will be unprofitable, and by 2050 40 percent—nearly half—of the health care providers will be unprofitable.

Again, in particularly rural communities, if you can't make it on the revenues that come from patients, from providing health care to individuals, often the option is to increase taxes—property taxes, sales tax—or something to keep your hospital doors open. That ought not be the consequence of legislation passed by Congress—to require taxes to be raised for a Federal program called Medicare because it is failing to meet the needs of American citizens, our patients. These providers, our hospitals, just simply can't sustain in the circumstance they find themselves in. The Affordable Care Act has put us on a path that I think is dangerous for individuals, for businesses, and now for the health care providers themselves.

In addition to the bad debt experience, many of the new health care plans have limited or restrictive provider networks, so that a local hospital may be eliminated from their network. This means that while under their previous insurance policy they could see a hometown physician or be admitted to their hometown hospital, because of these network restrictions they must go someplace out of town to access health care. This again is a terrible consequence for the individual, for the patient, but also something that drives revenues away from the hometown provider, much to the detriment of everybody who would want to make certain that provider, that doctor, remains in the community and that the hospital doors remain open.

There is lots of evidence that the problems we are facing are real. They demand attention. Access to affordable health care is something that still deserves our attention. I look forward to trying to make certain we have that opportunity. Again, that is nothing that is going to happen in the next few days, but we have a responsibility to see that the things that are reducing the access to affordable health care are addressed. The efforts that resulted from the Affordable Care Act are exacerbating the problem, not solving the problem.

I look at elections as like a new year. There is this optimism that maybe something good can come from a new Congress; that we can establish our New Year's resolutions and we can begin working, and I certainly make the offer to my colleagues throughout the Senate—all 99 of my colleagues—to be someone who wants to be problem solving, oriented toward finding solutions, and working together to make sure those health care providers that are so important to our lives, our safety, to our health, are around for a long time to come and that the communities that depend upon those hospitals—those 128 hospitals in my home State—have a viable future.

We have to get the regulatory environment under control, we have to resolve the problems created by the Affordable Care Act, and we need to make certain that health care is an opportunity for people who live in places across my State to still have the opportunity to see the hometown physician, to have a prescription filled by the hometown pharmacist, and to make certain those hometown hospital doors remain open for today and for future generations of communities across my State.

I appreciate the opportunity to address the Senate this afternoon, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. KING. I ask unanimous consent that the order for the quorum call be rescinded.

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

CYBERSECURITY ACT

Mr. KING. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 490, S. 1353.

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

The legislative clerk read as follows:

A bill (S. 1353) to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes.

There being no objection, the Senate proceeded to consider the bill, which had been reported from the Committee on Commerce, Science, and Transportation, with an amendment to strike all after the enacting clause and insert in lieu thereof the following:

S. 1353

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Cybersecurity Act of 2013''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) CYBERSECURITY MISSION.—The term ''cybersecurity mission'' means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) INFORMATION INFRASTRUCTURE.—The term ''information infrastructure'' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term in section 3502 of title 44, United States Code.

SEC. 3. NO REGULATORY AUTHORITY.

Nothing in this Act shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency.

TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

SEC. 101. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) CYBERSECURITY.—Section 2(c) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) is amended—

(1) by redesignating paragraphs (15) through (22) as paragraphs (16) through (23), respectively; and

(2) by inserting after paragraph (14) the following:

''(15) on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure (as defined under subsection (e));''.

(b) SCOPE AND LIMITATIONS.—Section 2 of the National Institute of Standards and Technology Act (15 U.S.C. 272) is amended by adding at the end the following:

''(e) CYBER RISKS.—

''(1) IN GENERAL.—In carrying out the activities under subsection (c)(15), the Director—

''(A) shall—

''(i) coordinate closely and continuously with relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations, and incorporate industry expertise;

''(ii) consult with the heads of agencies with national security responsibilities, sector-specific agencies, State and local governments, the governments of other nations, and international organizations;

''(iii) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks;

''(iv) include methodologies—

''(I) to identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

''(II) to protect individual privacy and civil liberties;

''(v) incorporate voluntary consensus standards and industry best practices;

''(vi) align with voluntary international standards to the fullest extent possible;

''(vii) prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes; and

''(viii) include such other similar and consistent elements as the Director considers necessary; and

''(B) shall not prescribe or otherwise require—

''(i) the use of specific solutions;

''(ii) the use of specific information or communications technology products or services; or

''(iii) that information or communications technology products or services be designed, developed, or manufactured in a particular manner.

''(2) LIMITATION.—Information shared with or provided to the Institute for the purpose of the activities described under subsection (c)(15) shall not be used by any Federal, State, tribal, or local department or agency to regulate the activity of any entity.

''(3) DEFINITIONS.—In this subsection:

''(A) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

''(B) SECTOR-SPECIFIC AGENCY.—The term 'sector-specific agency' means the Federal department or agency responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.''.

(c) STUDY AND REPORT.—

(1) STUDY.—The Comptroller General of the United States shall conduct a study that assesses—

(A) the progress made by the Director of the National Institute of Standards and Technology in facilitating the development of standards and procedures to reduce cyber risks to critical infrastructure in accordance with section 2(c)(15) of the National Institute of Standards and Technology Act, as added by this section;

(B) the extent to which the Director's facilitation efforts are consistent with the directive in such section that the development of such standards and procedures be voluntary and led by industry representatives;

(C) the extent to which sectors of critical infrastructure (as defined in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e))) have adopted a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure in accordance with such section 2(c)(15);

(D) the reasons behind the decisions of sectors of critical infrastructure (as defined in subparagraph (C)) to adopt or to not adopt the voluntary standards described in subparagraph (C); and

(E) the extent to which such voluntary standards have proved successful in protecting critical infrastructure from cyber threats.

(2) REPORTS.—Not later than 1 year after the date of the enactment of this Act, and every 2 years thereafter for the following 6 years, the Comptroller General shall submit a report, which summarizes the findings of the study conducted under paragraph (1), to—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Energy and Commerce of the House of Representatives; and

(C) the Committee on Science, Space, and Technology of the House of Representatives.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 201. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) FUNDAMENTAL CYBERSECURITY RESEARCH.—

(1) IN GENERAL.—The Director of the Office of Science and Technology Policy, in coordination with the head of any relevant Federal agency, shall build upon programs and plans in effect as of the date of enactment of this Act to develop a Federal cybersecurity research and development plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;

(D) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the growing problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services; and

(K) any additional objectives the Director of the Office of Science and Technology Policy, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determines appropriate.

(2) REQUIREMENTS.—

(A) IN GENERAL.—The Federal cybersecurity research and development plan shall identify and prioritize near-term, mid-term, and long-term research in computer and information science and engineering to meet the objectives under paragraph (1), including research in the areas described in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)).

(B) PRIVATE SECTOR EFFORTS.—In developing, implementing, and updating the Federal cybersecurity research and development plan, the Director of the Office of Science and Technology Policy shall work in close cooperation with industry, academia, and other interested stakeholders to ensure, to the extent possible, that Federal cybersecurity research and development is not duplicative of private sector efforts.

(3) TRIENNIAL UPDATES.—

(A) IN GENERAL.—The Federal cybersecurity research and development plan shall be updated triennially.

(B) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall submit the plan, not later than 1 year after the date of enactment of this Act, and

each updated plan under this section to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(b) CYBERSECURITY PRACTICES RESEARCH.—The Director of the National Science Foundation shall support research that—

(1) develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs; and

(2) develops new models for professional development of faculty in cybersecurity education, including secure coding development.

(c) CYBERSECURITY MODELING AND TEST BEDS.—

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Director the National Science Foundation, in coordination with the Director of the Office of Science and Technology Policy, shall conduct a review of cybersecurity test beds in existence on the date of enactment of this Act to inform the grants under paragraph (2). The review shall include an assessment of whether a sufficient number of cybersecurity test beds are available to meet the research needs under the Federal cybersecurity research and development plan.

(2) ADDITIONAL CYBERSECURITY MODELING AND TEST BEDS.—

(A) IN GENERAL.—If the Director of the National Science Foundation, after the review under paragraph (1), determines that the research needs under the Federal cybersecurity research and development plan require the establishment of additional cybersecurity test beds, the Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, may award grants to institutions of higher education or research and development non-profit institutions to establish cybersecurity test beds.

(B) REQUIREMENT.—The cybersecurity test beds under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real-time cyber attacks and defenses on real world networks and environments.

(C) ASSESSMENT REQUIRED.—The Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, shall evaluate the effectiveness of any grants awarded under this subsection in meeting the objectives of the Federal cybersecurity research and development plan under subsection (a) no later than 2 years after the review under paragraph (1) of this subsection, and periodically thereafter.

(d) COORDINATION WITH OTHER RESEARCH INITIATIVES.—In accordance with the responsibilities under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511), the Director the Office of Science and Technology Policy shall coordinate, to the extent practicable, Federal research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Science Foundation;

(2) the National Institute of Standards and Technology;

(3) the Department of Homeland Security;

(4) other Federal agencies;

(5) other Federal and private research laboratories, research entities, and universities;

(6) institutions of higher education;

(7) relevant nonprofit organizations; and

(8) international partners of the United States.

(e) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' at the end;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are integral to inter-network communications and data exchange;

''(K) secure software engineering and software assurance, including—

''(i) programming languages and systems that include fundamental security features;

''(ii) portable or reusable code that remains secure when deployed in various environments;

''(iii) verification and validation technologies to ensure that requirements and specifications have been implemented; and

''(iv) models for comparison and metrics to assure that required standards have been met;

''(L) holistic system security that—

''(i) addresses the building of secure systems from trusted and untrusted components;

''(ii) proactively reduces vulnerabilities;

''(iii) addresses insider threats; and

''(iv) supports privacy in conjunction with improved security;

''(M) monitoring and detection;

''(N) mitigation and rapid recovery methods;

''(O) security of wireless networks and mobile devices; and

''(P) security of cloud infrastructure and services.''.

(f) RESEARCH ON THE SCIENCE OF CYBERSECURITY.—The head of each agency and department identified under section 101(a)(3)(B) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)), through existing programs and activities, shall support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

SEC. 202. COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.

Section 4(b) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)) is amended—

(1) in paragraph (3), by striking ''the research areas'' and inserting the following: ''improving the security and resiliency of information infrastructure, reducing cyber vulnerabilities, and anticipating and mitigating consequences of cyber attacks on critical infrastructure, by conducting research in the areas'';

(2) by striking ''the center'' in paragraph (4)(D) and inserting ''the Center''; and

(3) in paragraph (5)—

(A) by striking ''and'' at the end of subparagraph (C);

(B) by striking the period at the end of subparagraph (D) and inserting a semicolon; and

(C) by adding at the end the following:

''(E) the demonstrated capability of the applicant to conduct high performance computation integral to complex computer and network security research, through on-site or off-site computing;

''(F) the applicant's affiliation with private sector entities involved with industrial research described in subsection (a)(1);

''(G) the capability of the applicant to conduct research in a secure environment;

''(H) the applicant's affiliation with existing research programs of the Federal Government;

''(I) the applicant's experience managing public-private partnerships to transition new technologies into a commercial setting or the government user community;

''(J) the capability of the applicant to conduct interdisciplinary cybersecurity research, basic and applied, such as in law, economics, or behavioral sciences; and

''(K) the capability of the applicant to conduct research in areas such as systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, or industrial control systems.''.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

SEC. 301. CYBERSECURITY COMPETITIONS AND CHALLENGES.

(a) IN GENERAL.—The Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, shall—

(1) support competitions and challenges under section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989) or any other provision of law, as appropriate—

(A) to identify, develop, and recruit talented individuals to perform duties relating to the security of information infrastructure in Federal, State, and local government agencies, and the private sector; or

(B) to stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that has the potential for application to the information technology activities of the Federal Government; and

(2) ensure the effective operation of the competitions and challenges under this section.

(b) PARTICIPATION.—Participants in the competitions and challenges under subsection (a)(1) may include—

(1) students enrolled in grades 9 through 12;

(2) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(3) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(4) institutions of higher education and research institutions;

(5) veterans; and

(6) other groups or individuals that the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security determine appropriate.

(c) AFFILIATION AND COOPERATIVE AGREEMENTS.—Competitions and challenges under this section may be carried out through affiliation and cooperative agreements with—

(1) Federal agencies;

(2) regional, State, or school programs supporting the development of cyber professionals;

(3) State, local, and tribal governments; or

(4) other private sector organizations.

(d) AREAS OF SKILL.—Competitions and challenges under subsection (a)(1)(A) shall be designed to identify, develop, and recruit exceptional talent relating to—

(1) ethical hacking;

(2) penetration testing;

(3) vulnerability assessment;

(4) continuity of system operations;

(5) security in design;

(6) cyber forensics;

(7) offensive and defensive cyber operations; and

(8) other areas the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security consider necessary to fulfill the cybersecurity mission.

(e) TOPICS.—In selecting topics for competitions and challenges under subsection (a)(1), the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security—

(1) shall consult widely both within and outside the Federal Government; and

(2) may empanel advisory committees.

(f) INTERNSHIPS.—The Director of the Office of Personnel Management may support, as appropriate, internships or other work experience in the Federal Government to the winners of the competitions and challenges under this section.

SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the

Director of the Office of Personnel Management and Secretary of Homeland Security, shall continue a Federal Cyber Scholarship-for-Service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The Federal Cyber Scholarship-for-Service program shall—

(1) provide scholarships to students who are enrolled in programs of study at institutions of higher education leading to degrees or specialized program certifications in the cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) provide a procedure by which the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, may request and fund security clearances for scholarship recipients, including providing for clearances during internships or other temporary appointments and after receipt of their degrees.

(c) SCHOLARSHIP AMOUNTS.—Each scholarship under subsection (b) shall be in an amount that covers the student's tuition and fees at the institution under subsection (b)(1) and provides the student with an additional stipend.

(d) SCHOLARSHIP CONDITIONS.—Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree.

(e) HIRING AUTHORITY.—

(1) APPOINTMENT IN EXCEPTED SERVICE.—Notwithstanding any provision of chapter 33 of title 5, United States Code, governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the academic program for which a scholarship was awarded.

(2) NONCOMPETITIVE CONVERSION.—Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) TIMING OF CONVERSION.—An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) AUTHORITY TO DECLINE CONVERSION.—An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

(f) ELIGIBILITY.—To be eligible to receive a scholarship under this section, an individual shall—

(1) be a citizen or lawful permanent resident of the United States;

(2) demonstrate a commitment to a career in improving the security of information infrastructure; and

(3) have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences.

(g) REPAYMENT.—If a scholarship recipient does not meet the terms of the program under this section, the recipient shall refund the scholarship payments in accordance with rules established by the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management and Secretary of Homeland Security.

(h) EVALUATION AND REPORT.—The Director of the National Science Foundation shall evaluate and report periodically to Congress on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector workforce.

SEC. 303. STUDY AND ANALYSIS OF EDUCATION, ACCREDITATION, TRAINING, AND CERTIFICATION OF INFORMATION INFRASTRUCTURE AND CYBERSECURITY PROFESSIONALS.

(a) STUDY.—The Director of the National Science Foundation, the Director of the Office of Personnel Management, and the Secretary of Homeland Security shall undertake to enter into appropriate arrangements with the National Academy of Sciences to conduct a comprehensive study of government, academic, and private-sector education, accreditation, training, and certification programs for the development of professionals in information infrastructure and cybersecurity. The agreement shall require the National Academy of Sciences to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of professionals in information infrastructure and cybersecurity should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector education, accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an evaluation of—

(A) the state of cybersecurity education at institutions of higher education in the United States;

(B) the extent of professional development opportunities for faculty in cybersecurity principles and practices;

(C) the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools;

(D) the proposed metrics to assess progress toward improving cybersecurity education; and

(E) the descriptions of the content of cybersecurity courses in undergraduate computer science curriculum;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(5) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academy of Sciences shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure and cybersecurity education, accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for further research and the improvement of information infrastructure and cybersecurity education, accreditation, training, and certification programs.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

SEC. 401. NATIONAL CYBERSECURITY AWARENESS AND PREPAREDNESS CAMPAIGN.

(a) NATIONAL CYBERSECURITY AWARENESS AND PREPAREDNESS CAMPAIGN.—The Director of the National Institute of Standards and Technology (referred to in this section as the ''Director''), in consultation with appropriate Federal agencies, shall continue to coordinate a national cybersecurity awareness and preparedness campaign, such as—

(1) a campaign to increase public awareness of cybersecurity, cyber safety, and cyber ethics, including the use of the Internet, social media, entertainment, and other media to reach the public;

(2) a campaign to increase the understanding of State and local governments, institutions of higher education, and private sector entities of—

(A) the benefits of ensuring effective risk management of the information infrastructure versus the costs of failure to do so; and

(B) the methods to mitigate and remediate vulnerabilities;

(3) support for formal cybersecurity education programs at all education levels to prepare skilled cybersecurity and computer science workers for the private sector and Federal, State, and local government; and

(4) initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal government and develop strategies for recruitment, training, and retention.

(b) CONSIDERATIONS.—In carrying out the authority described in subsection (a), the Director, in consultation with appropriate Federal agencies, shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently verified assessments regarding the quantification and valuation of information security risk.

(c) STRATEGIC PLAN.—The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of the date of enactment of this Act to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and preparedness campaign under subsection (a).

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, and every 5 years thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

IMPORTANT ASPECTS OF S. 1353

Mr. JOHNSON of South Dakota. Mr. President, I ask consent to engage in a colloquy with Senator ROCKEFELLER, Chairman of the Senate Commerce Committee, regarding important aspects of S. 1353, the Cybersecurity Enhancement Act of 2014.

Yesterday I held a hearing on the importance of improving information sharing between agencies on cyber security. As I said yesterday, law enforcement, the intelligence community, Treasury, and financial regulators each may have different missions, but in addressing cyber security concerns they all must be united in what some call a ''whole government'' approach. Cyber security is one of the most important issues facing the financial system and I hope next Congress can work together to pass a comprehensive cyber security bill. I thank my colleague, the Senator from West Virginia, for his work on this important matter and for strengthening the public-private collaboration on cyber security with this bill.

However, I would like to ensure that the language in this bill does not have

unintended consequences on the abilities of financial regulators to effectively oversee our financial system. As chairman of the Banking Committee, I am mindful of the importance of strong regulators examining and supervising our financial institutions. This is particularly important in the case of the Consumer Financial Protection Bureau, the agency that was created in 2010 to police areas of the financial market that previously were not regulated at the federal level, as well as the prudential regulators. A provision in S. 1353 states that information shared with the National Institute of Standards and Technology (known as NIST), may not be used by a government agency to regulate the activity of any entity. However, other existing statutes and regulations provide government agencies with the authority to require entities they regulate to provide them with information.

Moreover, a regulatory agency may discover such information on its own, through the entity, or through other sources. For example, a bank regulatory agency may discover cyberthreat information during a routine examination of a bank and, might want to exercise its existing legal authority to require the bank to adjust its systems to protect against future cyberthreats. I seek clarification from the Senator from West Virginia with respect to the provision in the proposed legislation.

Can my colleague from West Virginia confirm that this provision is not intended to prohibit an agency from taking regulatory action, if the agency independently obtains such information pursuant to other statutory or regulatory authority, even if a regulated entity has shared this information with NIST?

Mr. ROCKEFELLER. I thank Senator JOHNSON for his interest and support for this legislation and for his shared interest in strengthening cyber security. I also thank my colleague from South Dakota for drawing attention to the potential impact of this provision on financial regulatory authorities under the Banking Committee's jurisdiction, including those of the Consumer Financial Protection Bureau and the prudential regulators. I would like to assure the Senator that the consensus-based voluntary process for developing cyber security standards established in Title I of this bill is not intended to alter or limit financial regulatory agencies' regulatory authority in any way. Title I, particularly new section (e)(2) of the National Institute of Standards and Technology Act, encourages private entities to participate in NIST's standards development process, but is in no way a ''safe harbor'' for participants who are subject to the jurisdiction of financial regulatory agencies. An entity that participates in the standards development process established in Title I is still fully subject to the regulations, supervision, and other requirements of its financial regulatory agency. Sharing information with NIST as part of the process established in Title I is not a valid basis for withholding information from a regulator, including information about cyber threats.

NIST is the Federal government's premier science and standards agency. It is not a regulatory agency, nor is it a national or homeland security agency. NIST's unique role is to bring together knowledgeable players from government and industry and to build consensus around common technical standards. NIST has no authority to require any private entity to follow standards it develops. The cybersecurity standards development process established in Title I is therefore not a rulemaking process. It in no way imposes new or duplicative regulations on entities that are subject to the authority of financial regulatory agencies, and it in no way disturbs or diminishes agencies' authority to exercise their important oversight duties.

It is not intended to prohibit an agency from taking a regulatory action, such as an action to require an individual entity to protect against future cyber threats, if the agency independently obtains such information pursuant to other statutory or regulatory authority—even if an entity has shared this information with NIST. Nothing in this bill is intended to modify, limit, or otherwise affect the authority of the federal financial regulators under any other provision of law.

Mr. JOHNSON of South Dakota. I thank the Senator from West Virginia for his work on this important matter and for working with me to clarify the scope of this bill.

Mr. KING. I ask unanimous consent that the committee-reported substitute be agreed to, the Rockefeller-Thune substitute 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.

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

The committee-reported amendment in the nature of a substitute was agreed to.

The amendment (No. 4097) in the nature of a substitute was agreed to.

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

The bill (S. 1353), as amended, was ordered to be engrossed for a third reading, was read the third time, and passed.

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

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. SESSIONS. I ask unanimous consent that the order for the quorum call be rescinded.

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

PROTECTING VOLUNTEER FIREFIGHTERS AND EMERGENCY RESPONDERS ACT OF 2014—Continued

Mr. SESSIONS. Mr. President, I ask unanimous consent to speak as in morning business.

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

TRIBUTE TO DEPARTING SENATORS

TOM COBURN

Mr. SESSIONS. Mr. President, I would like to make some remarks about Senator COBURN.

TOM COBURN is one of the more remarkable Senators who have served in this body—certainly since I have been here. He is a man with absolute courage, conviction, and dedication to make this country better. He didn't come here to go through the job and go through the motions; he came here to invest his great skills and his great intellectual ability and to pour his drive and effort into making America a better place. It is very special. It is unusual. I have not seen anything like it, as I said, since I have been here.

I always had great reluctance to disagree or oppose anything Tom offered. They were not always perfect, but basically I opposed them so seldom because I agreed with him time and time again. I always hated to vote no because I knew he had studied the issue, understood it, and was doing what he believed was right.

His whole philosophy and approach to government, had it been more effectively followed by other Members of this body, would have led us to a better country. To support what he said, I think in a way, was supporting high ideals for America.

I want to say I am going to miss him. People have no idea how many times he has stopped or altered bad legislation to make it better and less problematic and more principled. He believes that ours is a constitutionally limited government. He didn't just believe that, he acted on it and has acted on it consistently.

I understand, and I have no doubt of this—we don't need to run a test—but I understand and have no doubt that he has offered more amendments since I have been in the Senate than any other Senator. They have been amendments to stop waste, fraud, and abuse, to make the government more efficient, leaner, to consolidate multiple programs that should be consolidated for efficiency.

He has worked across the aisle on a host of issues. He has sought bipartisan support for matters that are small and large. It is remarkable. I have to say that we are going to lose someone who is of great value. He would easily have been reelected had he run again.

I remember him saying one time—and this is his philosophy—if you want to be reelected, don't worry about being reelected, just do the right thing, and you won't have any difficulties. He never had any difficulties in his election, because people trusted him. They