Senator from Vermont (Mr. SANDERS) were added as cosponsors of amendment No. 1671 intended to be proposed to S. 1813, a bill to reauthorize Federal-aid highway and highway safety construction programs, and for other purposes.

AMENDMENT NO. 1702

At the request of Mr. CARPER, the names of the Senator from New Jersey (Mr. LAUTENBERG), the Senator from Rhode Island (Mr. WHITEHOUSE) and the Senator from Vermont (Mr. SANDERS) were added as cosponsors of amendment No. 1702 intended to be proposed to S. 1813, a bill to reauthorize Federal-aid highway and highway safety construction programs, and for other purposes.

AMENDMENT NO. 1743

At the request of Mr. BLUNT, the names of the Senator from South Carolina (Mr. DEMINT) and the Senator from Utah (Mr. LEE) were added as cosponsors of amendment No. 1743 intended to be proposed to S. 1813, a bill to reauthorize Federal-aid highway and highway safety construction programs, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. BINGAMAN (for himself, Mr. WYDEN, Mr. SANDERS, Mr. UDALL of Colorado, Mr. FRANKEN, Mr. COONS, Mr. KERRY, Mr. WHITEHOUSE, and Mr. UDALL of New Mexico):

S. 2146. A bill to amend the Public Utility Regulatory Policies Act of 1978 to create a market-oriented standard for clean electric energy generation, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. BINGAMAN. Mr. President, let me take a few minutes to describe this legislation for my colleagues and, hopefully, urge them to seriously consider the legislation. It is introduced by me with several cosponsors: Senator WYDEN, Senator SANDERS, Senator MARK UDALL of Colorado, Senator FRANKEN, Senator COONS, Senator KERRY, Senator WHITEHOUSE, and Senator TOM UDALL from my home State of New Mexico. All of those individuals strongly support what we are trying to do in this legislation.

I particularly want to thank the staff of the Senate Energy Committee for the hard work they put into developing this proposal, and particularly Kevin Rennert, who worked very hard on this proposal and got a lot of very useful input from many sectors and many individuals.

This is a simple plan to modernize the power sector and guide it toward a future in which more and more of our electricity is generated with cleaner and cleaner energy. The purpose of the legislation is to make sure that, as we continue to grow and power our economy, we leverage the clean resources we have available today and also provide a continuing incentive to develop the cheaper, cleaner technologies that will be needed in the future.

We want to make sure we drive continued diversity in our energy sources and allow every region of the country to deploy clean energy using the appropriate resources for that region. We want to make sure we do all of this in a way that supports homegrown innovation and manufacturing and that keeps us competitive in the global clean energy economy. The plan we are putting forward with this legislation would implement a clean energy standard, or CES for short.

Let me describe how it works. Starting in 2015, the largest utilities in the country would meet the clean energy standard by showing that a certain percentage of the electricity they sell is produced from clean energy sources. The initial percentage for 2015 is within the capabilities of those utilities today, and each year after 2015 they would be required to sell a little bit more of their electricity from clean sources. They can do so either by making incremental adjustments to their own energy mix to become cleaner and more efficient or by purchasing clean energy from those who provide it at the lowest cost or by purchasing credits on an open and transparent market.

To be considered clean, a generator must either be a zero carbon source of energy, such as, renewables and nuclear power, or a generator must have a lower carbon intensity than a modern, efficient coal plant. By carbon intensity, I mean the amount of carbon dioxide emitted per megawatt hour of electricity generated. Generators with low or no carbon intensity receive credits based on that criterion.

For example, renewables will receive a full credit per megawatt hour. Most natural gas generators would qualify for something around a half credit, and the more efficient natural gas generators would be incentivized compared to less efficient generators. A coal powerplant would receive some credits if it lowered its carbon intensity by installing carbon-capture technologies, by cofiring with renewable biomass.

Accounting for clean in this way means the cleanest resources have the greatest incentive. Also, it means every generator has a continuing incentive to become even more efficient. As the standard increases over time, the generation fleet will transition naturally toward cleaner and cleaner sources to meet it. The clean energy standard sets an overall goal for clean energy, but the optimal and the cheapest set of technologies to use will be determined by the free market. The rate of transition is predictable and it is achievable and the rules of the road are transparent and they are clear.

In addition to driving cleaner electricity generation in the power sector, the clean energy standard also rewards industrial efficiency. Combined heat and power units generate electricity while also capturing and using the heat for other purposes, and these units are treated as clean generators under this proposal for the clean energy standard. This will help to deploy this kind of efficiency throughout our country and will provide another source of inexpensive clean energy.

Let me also describe what this proposal does not do. The clean energy standard does not put a limit on overall emissions. It does not limit the growth of electricity generation to meet the demands of a growing economy. All that the clean energy standard requires is that the generation we do use in future years and that we add to our fleet gradually becomes cleaner over time.

The clean energy standard does not cost the government anything, and it does not raise money for the government to use either. If any money does come to the Treasury as a result of the program because of refusal to participate or to comply, that money would go directly back to the particular State from which it came to fund energy-efficiency programs.

Finally, the clean energy standard will not hurt the economy. This past fall I asked the Energy Information Administration to analyze a number of clean energy standard policy options. The results of their study showed a properly designed clean energy standard would have almost zero impact on gross domestic product growth and little or no impact on nationally averaged electricity rates for the first decade of the program. The Energy Information Administration analysis did show that a clean energy standard would result in a substantial deployment of new clean energy and carbon reductions between 20 percent and 40 percent in the power sector by 2035, which is the timeframe provided for in the proposal.

I have asked the Energy Information Administration to update their modeling to reflect this final proposal that we are introducing today, and when they have completed that analysis in the next few weeks I plan to hold hearings on the proposal to further explore the benefits and effects of the clean energy standard in the Energy Committee.

The goal of the clean energy standard is ambitious. It is a doubling of clean energy production in this country by 2035. But analysis has shown that the goal is achievable and affordable. Meeting the clean energy standard will yield substantial benefits to our health and to our economy and to our global competitiveness, and, of course, to our environment.

The bill we are introducing today is simple. It sets a national goal for clean energy. It establishes a transparent framework that lets resources compete to achieve that goal based on how clean they are, and then it gets out of the way and lets the market and American ingenuity determine the best path forward.

I think this is a very well thought out proposal and one that deserves the

attention of all colleagues. I hope they will look at it seriously, and I hope we can attract additional supporters and cosponsors as the weeks proceed in the Senate.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 2146

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Clean Energy Standard Act of 2012''.

SEC. 2. FEDERAL CLEAN ENERGY STANDARD.

Title VI of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2601 et seq.) is amended by adding at the end the following:

''SEC. 610. FEDERAL CLEAN ENERGY STANDARD.

''(a) PURPOSE.—The purpose of this section is to create a market-oriented standard for electric energy generation that stimulates clean energy innovation and promotes a diverse set of low- and zero-carbon generation solutions in the United States at the lowest incremental cost to electric consumers.

''(b) DEFINITIONS.—In this section:

''(1) CLEAN ENERGY.—The term 'clean energy' means electric energy that is generated—

''(A) at a facility placed in service after December 31, 1991, using—

''(i) renewable energy;

''(ii) qualified renewable biomass;

''(iii) natural gas;

''(iv) hydropower;

''(v) nuclear power; or

''(vi) qualified waste-to-energy;

''(B) at a facility placed in service after the date of enactment of this section, using—

''(i) qualified combined heat and power; or

''(ii) a source of energy, other than biomass, with lower annual carbon intensity than 0.82 metric tons of carbon dioxide equivalent per megawatt-hour;

''(C) as a result of qualified efficiency improvements or capacity additions; or

''(D) at a facility that captures carbon dioxide and prevents the release of the carbon dioxide into the atmosphere.

''(2) NATURAL GAS.—

''(A) INCLUSION.—The term 'natural gas' includes coal mine methane.

''(B) EXCLUSIONS.—The term 'natural gas' excludes landfill methane and biogas.

''(3) QUALIFIED COMBINED HEAT AND POWER.—

''(A) IN GENERAL.—The term 'qualified combined heat and power' means a system that—

''(i) uses the same energy source for the simultaneous or sequential generation of electrical energy and thermal energy;

''(ii) produces at least—

''(I) 20 percent of the useful energy of the system in the form of electricity; and

''(II) 20 percent of the useful energy in the form of useful thermal energy;

''(iii) to the extent the system uses biomass, uses only qualified renewable biomass; and

''(iv) operates with an energy efficiency percentage that is greater than 50 percent.

''(B) DETERMINATION OF ENERGY EFFICIENCY.—For purposes of subparagraph (A), the energy efficiency percentage of a combined heat and power system shall be determined in accordance with section 48(c)(3)(C)(i) of the Internal Revenue Code of 1986.

''(4) QUALIFIED EFFICIENCY IMPROVEMENTS OR CAPACITY ADDITIONS.—

''(A) IN GENERAL.—Subject to subparagraphs (B) and (C), the term 'qualified efficiency improvements or capacity additions' means efficiency improvements or capacity additions made after December 31, 1991, to—

''(i) a nuclear facility placed in service on or before December 31, 1991; or

''(ii) a hydropower facility placed in service on or before December 31, 1991.

''(B) EXCLUSION.—The term 'qualified efficiency improvements or capacity additions' does not include additional electric energy generated as a result of operational changes not directly associated with efficiency improvements or capacity additions.

''(C) MEASUREMENT AND CERTIFICATION.—In the case of hydropower, efficiency improvements and capacity additions under this paragraph shall be—

''(i) measured on the basis of the same water flow information that is used to determine the historic average annual generation for the applicable hydroelectric facility; and

''(ii) certified by the Secretary or the Commission.

''(5) QUALIFIED RENEWABLE BIOMASS.—The term 'qualified renewable biomass' means renewable biomass produced and harvested through land management practices that maintain or restore the composition, structure, and processes of ecosystems, including the diversity of plant and animal communities, water quality, and the productive capacity of soil and the ecological systems.

''(6) QUALIFIED WASTE-TO-ENERGY.—The term 'qualified waste-to-energy' means energy produced—

''(A) from the combustion of—

''(i) post-recycled municipal solid waste;

''(ii) gas produced from the gasification or pyrolization of post-recycled municipal solid waste;

''(iii) biogas;

''(iv) landfill methane;

''(v) animal waste or animal byproducts; or

''(vi) wood, paper products that are not commonly recyclable, and vegetation (including trees and trimmings, yard waste, pallets, railroad ties, crates, and solid-wood manufacturing and construction debris), if diverted from or separated from other waste out of a municipal waste stream; and

''(B) at a facility that the Commission has certified, on an annual basis, is in compliance with all applicable Federal and State environmental permits, including—

''(i) in the case of a facility that commences operation before the date of enactment of this section, compliance with emission standards under sections 112 and 129 of the Clean Air Act (42 U.S.C. 7412, 7429) that apply as of the date of enactment of this section to new facilities within the applicable source category; and

''(ii) in the case of a facility that produces electric energy from the combustion, pyrolization, or gasification of municipal solid waste, certification that each local government unit from which the waste originates operates, participates in the operation of, contracts for, or otherwise provides for recycling services for residents of the local government unit.

''(7) RENEWABLE ENERGY.—The term 'renewable energy' means solar, wind, ocean, current, wave, tidal, or geothermal energy.

''(c) CLEAN ENERGY REQUIREMENT.—

''(1) IN GENERAL.—Effective beginning in calendar year 2015, each electric utility that sells electric energy to electric consumers in a State shall obtain a percentage of the electric energy the electric utility sells to electric consumers during a calendar year from clean energy.

''(2) PERCENTAGE REQUIRED.—The percentage of electric energy sold during a calendar year that is required to be clean energy under paragraph (1) shall be determined in accordance with the following table:

''Calendar year	Minimum annual percentage
2015	24
2016	27
2017	30
2018	33
2019	36
2020	39
2021	42
2022	45
2023	48
2024	51
2025	54
2026	57
2027	60
2028	63
2029	66
2030	69
2031	72
2032	75
2033	78
2034	81
2035	84

''(3) DEDUCTION FOR ELECTRIC ENERGY GENERATED FROM HYDROPOWER OR NUCLEAR POWER.—An electric utility that sells electric energy to electric consumers from a facility placed in service in the United States on or before December 31, 1991, using hydropower or nuclear power may deduct the quantity of the electric energy from the quantity to which the percentage in paragraph (2) applies.

''(d) MEANS OF COMPLIANCE.—An electric utility shall meet the requirements of subsection (c) by—

''(1) submitting to the Secretary clean energy credits issued under subsection (e);

''(2) making alternative compliance payments of 3 cents per kilowatt hour in accordance with subsection (i); or

''(3) taking a combination of actions described in paragraphs (1) and (2).

''(e) FEDERAL CLEAN ENERGY TRADING PROGRAM.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this section, the Secretary shall establish a Federal clean energy credit trading program under which electric utilities may submit to the Secretary clean energy credits to certify compliance by the electric utilities with subsection (c).

''(2) CLEAN ENERGY CREDITS.—Except as provided in paragraph (3)(B), the Secretary shall issue to each generator of electric energy a quantity of clean energy credits determined in accordance with subsections (f) and (g).

''(3) ADMINISTRATION.—In carrying out the program under this subsection, the Secretary shall ensure that—

''(A) a clean energy credit shall be used only once for purposes of compliance with this section; and

''(B) a clean energy credit issued for clean energy generated and sold for resale under a contract in effect on the date of enactment of this section shall be issued to the purchasing electric utility, unless otherwise provided by the contract.

''(4) DELEGATION OF MARKET FUNCTION.—

''(A) IN GENERAL.—In carrying out the program under this subsection, the Secretary may delegate—

''(i) to 1 or more appropriate market-making entities, the administration of a national clean energy credit market for purposes of establishing a transparent national market for the sale or trade of clean energy credits; and

''(ii) to appropriate entities, the tracking of dispatch of clean generation.

''(B) ADMINISTRATION.—In making a delegation under subparagraph (A)(ii), the Secretary shall ensure that the tracking and reporting of information concerning the dispatch of clean generation is transparent, verifiable, and independent of any generation or load interests subject to an obligation under this section.

''(5) BANKING OF CLEAN ENERGY CREDITS.—Clean energy credits to be used for compliance purposes under subsection (c) shall be valid for the year in which the clean energy credits are issued or in any subsequent calendar year.

''(f) DETERMINATION OF QUANTITY OF CREDIT.—

''(1) IN GENERAL.—Except as otherwise provided in this subsection, the quantity of clean energy credits issued to each electric utility generating electric energy in the United States from clean energy shall be equal to the product of—

''(A) for each generator owned by a utility, the number of megawatt-hours of electric energy sold from that generator by the utility; and

''(B) the difference between—

''(i) 1.0; and

''(ii) the quotient obtained by dividing—

''(I) the annual carbon intensity of the generator, as determined in accordance with subsection (g), expressed in metric tons per megawatt-hour; by

''(II) 0.82.

''(2) NEGATIVE CREDITS.—Notwithstanding any other provision of this subsection, the Secretary shall not issue a negative quantity of clean energy credits to any generator.

''(3) QUALIFIED COMBINED HEAT AND POWER.—

''(A) IN GENERAL.—The quantity of clean energy credits issued to an owner of a qualified combined heat and power system in the United States shall be equal to the difference between—

''(i) the product obtained by multiplying—

''(I) the number of megawatt-hours of electric energy generated by the system; and

''(II) the difference between—

''(aa) 1.0; and

''(bb) the quotient obtained by dividing—

''(AA) the annual carbon intensity of the generator, as determined in accordance with subsection (g), expressed in metric tons per megawatt-hour; by

''(BB) 0.82; and

''(ii) the product obtained by multiplying—

''(I) the number of megawatt-hours of electric energy generated by the system that are consumed onsite by the facility; and

''(II) the annual target for electric energy sold during a calendar year that is required to be clean energy under subsection (c)(2).

''(B) ADDITIONAL CREDITS.—In addition to credits issued under subparagraph (A), the Secretary shall award clean energy credits to an owner of a qualified heat and power system in the United States for greenhouse gas emissions avoided as a result of the use of a qualified combined heat and power system, rather than a separate thermal source, to meet onsite thermal needs.

''(4) QUALIFIED WASTE-TO-ENERGY.—The quantity of clean energy credits issued to an electric utility generating electric energy in the United States from a qualified waste-to-energy facility shall be equal to the product obtained by multiplying—

''(A) the number of megawatt-hours of electric energy generated by the facility and sold by the utility; and

''(B) 1.0.

''(g) DETERMINATION OF ANNUAL CARBON INTENSITY OF GENERATING FACILITIES.—

''(1) IN GENERAL.—For purposes of determining the quantity of credits under subsection (f), except as provided in paragraph (2), the Secretary shall determine the annual carbon intensity of each generator by dividing—

''(A) the net annual carbon dioxide equivalent emissions of the generator; by

''(B) the annual quantity of electricity generated by the generator.

''(2) BIOMASS.—The Secretary shall—

''(A) not later than 180 days after the date of enactment of this section, issue interim regulations for determining the carbon intensity based on an initial consideration of the issues to be reported on under subparagraph (B);

''(B) not later than 180 days after the date of enactment of this section, enter into an agreement with the National Academy of Sciences under which the Academy shall—

''(i) evaluate models and methodologies for quantifying net changes in greenhouse gas emissions associated with generating electric energy from each significant source of qualified renewable biomass, including evaluation of additional sequestration or emissions associated with changes in land use by the production of the biomass; and

''(ii) not later than 1 year after the date of enactment of this section, publish a report that includes—

''(I) a description of the evaluation required by clause (i); and

''(II) recommendations for determining the carbon intensity of electric energy generated from qualified renewable biomass under this section; and

''(C) not later than 180 days after the publication of the report under subparagraph (B)(ii), issue regulations for determining the carbon intensity of electric energy generated from qualified renewable biomass that take into account the report.

''(3) CONSULTATION.—The Secretary shall consult with—

''(A) the Administrator of the Environmental Protection Agency in determining the annual carbon intensity of generating facilities under paragraph (1); and

''(B) the Administrator of the Environmental Protection Agency, the Secretary of the Interior, and the Secretary of Agriculture in issuing regulations for determining the carbon intensity of electric energy generated by biomass under paragraph (2)(C).

''(h) CIVIL PENALTIES.—

''(1) IN GENERAL.—Subject to paragraph (2), an electric utility that fails to meet the requirements of this section shall be subject to a civil penalty in an amount equal to the product obtained by multiplying—

''(A) the number of kilowatt-hours of electric energy sold by the utility to electric consumers in violation of subsection (c); and

''(B) 200 percent of the value of the alternative compliance payment, as adjusted under subsection (m).

''(2) WAIVERS AND MITIGATION.—

''(A) FORCE MAJEURE.—The Secretary may mitigate or waive a civil penalty under this subsection if the electric utility was unable to comply with an applicable requirement of this section for reasons outside of the reasonable control of the utility.

''(B) REDUCTION FOR STATE PENALTIES.—The Secretary shall reduce the amount of a penalty determined under paragraph (1) by the amount paid by the electric utility to a State for failure to comply with the requirement of a State renewable energy program, if the State requirement is more stringent than the applicable requirement of this section.

''(3) PROCEDURE FOR ASSESSING PENALTY.—The Secretary shall assess a civil penalty under this subsection in accordance with section 333(d) of the Energy Policy and Conservation Act (42 U.S.C. 6303(d)).

''(i) ALTERNATIVE COMPLIANCE PAYMENTS.—An electric utility may satisfy the requirements of subsection (c), in whole or in part, by submitting in lieu of a clean energy credit issued under this section a payment equal to the amount required under subsection (d)(2), in accordance with such regulations as the Secretary may promulgate.

''(j) STATE ENERGY EFFICIENCY FUNDING PROGRAM.—

''(1) ESTABLISHMENT.—Not later than December 31, 2015, the Secretary shall establish a State energy efficiency funding program.

''(2) FUNDING.—All funds collected by the Secretary as alternative compliance payments under subsection (i), or as civil penalties under subsection (h), shall be used solely to carry out the program under this subsection.

''(3) DISTRIBUTION TO STATES.—

''(A) IN GENERAL.—An amount equal to 75 percent of the funds described in paragraph (2) shall be used by the Secretary, without further appropriation or fiscal year limitation, to provide funds to States for the implementation of State energy efficiency plans under section 362 of the Energy Policy and Conservation Act (42 U.S.C. 6322), in accordance with the proportion of those amounts collected by the Secretary from each State.

''(B) ACTION BY STATES.—A State that receives funds under this paragraph shall maintain such records and evidence of compliance as the Secretary may require.

''(4) GUIDELINES AND CRITERIA.—The Secretary may issue such additional guidelines and criteria for the program under this subsection as the Secretary determines to be appropriate.

''(k) EXEMPTIONS.—

''(1) IN GENERAL.—This section shall not apply during any calendar year to an electric utility that sold less than the applicable quantity described in paragraph (2) of megawatt-hours of electric energy to electric consumers during the preceding calendar year.

''(2) APPLICABLE QUANTITY.—For purposes of paragraph (1), the applicable quantity is—

''(A) in the case of calendar year 2015, 2,000,000;

''(B) in the case of calendar year 2016, 1,900,000;

''(C) in the case of calendar year 2017, 1,800,000;

''(D) in the case of calendar year 2018, 1,700,000;

''(E) in the case of calendar year 2019, 1,600,000;

''(F) in the case of calendar year 2020, 1,500,000;

''(G) in the case of calendar year 2021, 1,400,000;

''(H) in the case of calendar year 2022, 1,300,000;

''(I) in the case of calendar year 2023, 1,200,000;

''(J) in the case of calendar year 2024, 1,100,000; and

''(K) in the case of calendar year 2025 and each calendar year thereafter, 1,000,000.

''(3) CALCULATION OF ELECTRIC ENERGY SOLD.—

''(A) DEFINITIONS.—In this subsection, the terms 'affiliate' and 'associate company' have the meanings given the terms in section 1262 of the Energy Policy Act of 2005 (42 U.S.C. 16451).

''(B) INCLUSION.—For purposes of calculating the quantity of electric energy sold by an electric utility under this subsection, the quantity of electric energy sold by an affiliate of the electric utility or an associate company shall be treated as sold by the electric utility.

''(l) STATE PROGRAMS.—

''(1) SAVINGS PROVISION.—

''(A) IN GENERAL.—Subject to paragraph (2), nothing in this section affects the authority of a State or a political subdivision of a State to adopt or enforce any law or regulation relating to—

''(i) clean or renewable energy; or

''(ii) the regulation of an electric utility.

''(B) FEDERAL LAW.—No law or regulation of a State or a political subdivision of a State may relieve an electric utility from compliance with an applicable requirement of this section.

''(2) COORDINATION.—The Secretary, in consultation with States that have clean and renewable energy programs in effect, shall facilitate, to the maximum extent practicable, coordination between the Federal clean energy program under this section and the relevant State clean and renewable energy programs.

''(m) ADJUSTMENT OF ALTERNATIVE COMPLIANCE PAYMENT.—Not later than December 31, 2016, and annually thereafter, the Secretary shall—

''(1) increase by 5 percent the rate of the alternative compliance payment under subsection (d)(2); and

''(2) additionally adjust that rate for inflation, as the Secretary determines to be necessary.

''(n) REPORT ON CLEAN ENERGY RESOURCES THAT DO NOT GENERATE ELECTRIC ENERGY.—

''(1) IN GENERAL.—Not later than 3 years after the date of enactment of this section, the Secretary shall submit to Congress a report examining mechanisms to supplement the standard under this section by addressing clean energy resources that do not generate electric energy but that may substantially reduce electric energy loads, including energy efficiency, biomass converted to thermal energy, geothermal energy collected using heat pumps, thermal energy delivered through district heating systems, and waste heat used as industrial process heat.

''(2) POTENTIAL INTEGRATION.—The report under paragraph (1) shall examine the benefits and challenges of integrating the additional clean energy resources into the standard established by this section, including—

''(A) the extent to which such an integration would achieve the purposes of this section;

''(B) the manner in which a baseline describing the use of the resources could be developed that would ensure that only incremental action that increased the use of the resources received credit; and

''(C) the challenges of pricing the resources in a comparable manner between organized markets and vertically integrated markets, including options for the pricing.

''(3) COMPLEMENTARY POLICIES.—The report under paragraph (1) shall examine the benefits and challenges of using complementary policies or standards, other than the standard established under this section, to provide effective incentives for using the additional clean energy resources.

''(4) LEGISLATIVE RECOMMENDATIONS.—As part of the report under paragraph (1), the Secretary may provide legislative recommendations for changes to the standard established under this section or new complementary policies that would provide effective incentives for using the additional clean energy resources.

''(o) EXCLUSIONS.—This section does not apply to an electric utility located in the State of Alaska or Hawaii.

''(p) REGULATIONS.—Not later than 1 year after the date of enactment of this section, the Secretary shall promulgate regulations to implement this section.

''SEC. 611. REPORT ON NATURAL GAS CONSERVATION.

''Not later than 2 years after the date of enactment of this section, the Secretary shall submit to Congress a report that—

''(1) quantifies the losses of natural gas during the production and transportation of the natural gas; and

''(2) makes recommendations, as appropriate, for programs and policies to promote conservation of natural gas for beneficial use.''.

By Mr. BEGICH:

S. 2147. A bill to provide for research, monitoring, and observation of the Arctic Ocean and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mr. BEGICH. Mr. President, I wish to speak about legislation I am introducing today aimed at providing a better understanding of the Arctic Ocean and its resources.

A changing climate is radically reshaping this part of the world. This change brings challenges and opportunities. As you may recall, nearly 3 years ago, I delivered my first speech to this body on the changing Arctic and what our Nation needs to do in order to prepare for it. That work continues today.

Retreating sea ice is leading to dramatic increases in shipping traffic of both goods and tourists. Our Nation's energy needs demand we investigate and responsibly produce the massive amounts of oil and gas found in the Chukchi and Beaufort Seas. These resources are now available due to retreating sea ice, the state of technology and the price of oil. Meanwhile, Native Alaskans have depended on and thrived for thousands of years because of the living resources of the Arctic Ocean.

In order to manage this change, we need a better understanding of the Arctic Ocean, and the legislation I am introducing today provides a firm foundation for that work. It establishes a new coherent research strategy to gather baseline information and to provide a holistic look at the Arctic Ocean.

Importantly, it doesn't create any new bureaucracy. It assigns this task to the North Pacific Research Board, a well regarded institution, and requires a high degree of coordination with other existing entities, including the Arctic Research Commission whose job it is to establish Arctic research priorities and coordinate the massive federal investment in this area across many agencies.

I would argue that most people are unaware of just how much Arctic science and research is underway. For most people in the lower 48 States, it is out-of-sight and out-of-mind. The Bureau of Ocean Energy Management has spent about half of its total research budget on the Arctic for the past 6 years, approximately $60 million. The National Science Foundation has spent more.

However, the Arctic Ocean Research, Monitoring, and Observing Act will be important to provide funds not tied to particular projects. This legislation is intended to provide a firm foundation in our understanding of the basic science of the Arctic Ocean that can underlie all of our decision-making in the Arctic.

I am always happy to inform my colleagues about how we do things right in Alaska. We're a natural resource development state. Because our economy is so dependent on that development, we bear the responsibility of doing it right. That is making sure that nonrenewable resource development doesn't harm the renewable resources of our great state.

I am confident we can continue to do that as we explore and develop the approximately 26 billion barrels of oil and 100 trillion cubic feet of natural gas in the Chukchi and Beaufort Seas. However, we have to make prudent investments in order to meet that goal, and that is what I am suggesting we do today.

With companion legislation I will be introducing in the next few days, I also have a plan to create an endowment to fund this critical research program. Baseline science and monitoring requires steady, dependable funding in order to have the long term data sets that can help us make good decisions. I look forward to working with my colleagues and the administration on this important need.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 2147

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Arctic Ocean Research, Monitoring, and Observing Act of 2012''.

SEC. 2. FINDINGS AND PURPOSE.

(a) FINDINGS.—Congress makes the following findings:

(1) The United States is an Arctic Nation with—

(A) an approximately 700-mile border with the Arctic Ocean;

(B) more than 100,000,000 acres of land above the Arctic Circle; and

(C) an even broader area defined as Arctic by temperature, which includes the Bering Sea and Aleutian Islands.

(2) The Arctic region of the United States is home to an indigenous population that has subsisted for millennia on the abundance in marine mammals, fish, and wildlife, many of which are unique to the region.

(3) Temperatures in the United States Arctic region have warmed by 3 to 4 degrees Celsius over the past half-century, a rate of increase that is twice the global average.

(4) The Arctic ice pack is rapidly diminishing and thinning, and the National Oceanic and Atmospheric Administration estimates the Arctic Ocean may be ice free during summer months in as few as 30 years.

(5) Such changes to the Arctic region are having a significant impact on the indigenous people of the Arctic, their communities and ecosystems, as well as the marine mammals, fish, and wildlife upon which they depend.

(6) Such changes are opening new portions of the United States Arctic continental shelf to possible development for offshore oil and gas, commercial fishing, marine shipping, and tourism.

(7) Existing Federal research and science advisory programs focused on the environmental and socioeconomic impacts of a changing Arctic Ocean lack a cohesive, coordinated, and integrated approach and are not adequately coordinated with State, local, academic, and private-sector Arctic Ocean research programs.

(8) The lack of research integration and synthesis of findings of Arctic Ocean research has impeded the progress of the United States and international community in understanding climate change impacts and feedback mechanisms in the Arctic Ocean.

(9) An improved scientific understanding of the changing Arctic Ocean is critical to the development of appropriate and effective regional, national, and global climate change adaptation strategies.

(b) PURPOSE.—The purpose of this Act is to establish a permanent environmental sentinel program to conduct research, monitoring, and observation activities in the Arctic Ocean—

(1) to promote and sustain a productive and resilient marine, coastal, and estuarine ecosystem in the Arctic and the human uses of its natural resources through greater understanding of how the ecosystem works and monitoring and observation of its vital signs; and

(2) to track and evaluate the effectiveness of natural resource management in the Arctic in order to facilitate improved performance and adaptive management.

SEC. 3. DEFINITIONS.

In this Act:

(1) BOARD.—The term ''Board'' means the North Pacific Research Board established under section 401(e) of the Department of the Interior and Related Agencies Appropriations Act, 1998 (Public Law 105–1608).

(2) COMMISSION.—The term ''Commission'' means the Arctic Research Commission established under the Arctic Research and Policy Act of 1984 (Public Law 98–373; 15 U.S.C. 4102).

(3) PROGRAM.—The term ''Program'' means the Arctic Ocean Research, Monitoring, and Observation Program established by section 4(a).

SEC. 4. ARCTIC OCEAN RESEARCH, MONITORING, AND OBSERVATION PROGRAM.

(a) ESTABLISHMENT.—There is established an Arctic Ocean Research, Monitoring, and Observation Program to be administered by the Board with input and assistance from the Commission.

(b) RESEARCH, MONITORING, AND OBSERVATION ACTIVITIES.—The Program shall be an integrated, long-term scientific research, monitoring, and observation program consisting of—

(1) marine, coastal, and estuarine research, including—

(A) fisheries research;

(B) research on the structure and function of the ecosystem and its food webs; and

(C) research on the spatial distributions and status of fish, wildlife, and other populations in the Arctic;

(2) marine, coastal, and estuarine ecosystem monitoring and observation, including expansion of the Alaska Ocean Observing System in the Arctic; and

(3) marine, coastal, and estuarine research, monitoring, observation, and modeling that supports planning, environmental review, decisionmaking, evaluation, impact and natural resources damage assessment, and adaptive management with respect to industrial and other human activities, such as shipping, in the Arctic, environmental change, and their interactive and cumulative effects in the Arctic.

(c) INITIAL PROJECTS.—In initiating the Program, the Board shall make grants under subsection (e)—

(1) to support research and monitoring of Arctic fisheries, including on the distributions and ecology of Arctic cod and other forage fishes, for a period of not less than 3 years;

(2) to support research and monitoring of Arctic marine mammals, including their responses to loss of sea ice habitats and reactions to disturbance, for a period of not less than 3 years; and

(3) to establish the Alaska Ocean Observing System in the Arctic Ocean such that it has sufficient capacity to provide comprehensive data, nowcasts and forecasts, and information products in real time and near real time on physical, chemical, and biological conditions and environmental change.

(d) ARCTIC OCEAN SCIENCE PLAN.—

(1) REQUIREMENT.—The Board and the Commission shall jointly prepare a comprehensive, integrated Arctic Ocean science plan.

(2) RECOGNITION AND COORDINATION WITH OTHER SCIENCE.—The content of the plan required by paragraph (1) shall be developed with recognition of and in coordination with other science plans and activities in the Arctic.

(3) INFORMED BY SYNTHESIS OF EXISTING KNOWLEDGE.—Development of the plan required by paragraph (1) shall be informed by a synthesis of existing knowledge about the Arctic ecosystem, including information about how the ecosystem functions, individual and cumulative sources of ecosystem stress, how the ecosystem is changing, and other relevant information.

(4) REVIEW.—

(A) INITIAL REVIEW BY NATIONAL RESEARCH COUNCIL.—The Board shall submit the initial plan required by paragraph (1) to the National Research Council for review.

(B) PERIODIC REVIEW AND UPDATES.—Not less frequently than once every 5 years thereafter, the Board and the Commission shall, in consultation with the National Research Council, review the plan required by paragraph (1) and update it as the Board and the Commission consider necessary.

(5) USE.—The Board shall use the plan required by paragraph (1) as a basis for setting priorities and awarding grants under subsection (e).

(e) GRANTS.—

(1) AUTHORITY.—Except as provided in paragraph (2), the Board shall, under the Program, award grants to carry out research, monitoring, and observation activities described in subsections (b) and (c).

(2) LIMITATION.—The North Pacific Research Board may not award any grants under paragraph (1) until the Board has prepared the plan required by subsection (d)(1).

(3) CONDITIONS, CONSIDERATIONS, AND PRIORITIES.—When making grants to carry out the research, monitoring, and observation activities described in subsections (b) and (c), the Board shall—

(A) consider institutions located in the Arctic and subarctic;

(B) place a priority on cooperative, integrated long-term projects, designed to address current or anticipated marine ecosystem or fishery or wildlife management information needs;

(C) give priority to fully establishing and operating the Alaska Ocean Observing System in the Arctic Ocean, which may include future support for cabled ocean observatories;

(D) recognize the value of local and traditional ecological knowledge, and, where appropriate, place a priority on research, monitoring, and observation projects that incorporate local and traditional ecological knowledge;

(E) ensure that research, monitoring, and observation data collected by grantees of the Program are made available to the public in a timely fashion, pursuant to national and international protocols; and

(F) give due consideration to the annual recommendations and review of the Commission carried out under subsection (f).

(f) ANNUAL RECOMMENDATIONS AND REVIEW BY ARCTIC RESEARCH COMMISSION.—Each year, the Commission shall—

(1) recommend ongoing and future research, monitoring, and observation priorities and strategies to be carried out pursuant to subsections (b) and (c);

(2) undertake a written review of ongoing and recently concluded research, monitoring, and observation activities undertaken pursuant to such subsections; and

(3) submit to the Board the recommendations required by paragraph (1) and the review required by paragraph (2).

By Ms. SNOWE:

S. 2150. A bill to amend title XVI of the Social Security Act to clarify that the value of certain funeral and burial arrangements are not to be considered available resources under the supplemental security income program; to the Committee on Finance.

Ms. SNOWE. Mr. President, I rise today to introduce valuable, bipartisan legislation that would codify the current policy of the Social Security Administration, SSA, to protect access to the Supplemental Security Income, SSI, program for those who prepay burial and funeral expenses.

When individuals are fiscally responsible, and plan ahead for their end-of-life costs, it makes no sense to penalize them. Under the current policy, if funds or life insurance are set aside, irrevocably—so the individual cannot take them back even if he or she wants to—then those resources do not count against the individual when determining whether or not they are eligible for SSI. This is a good policy, and I applaud the SSA for maintaining it.

Regrettably, this has not always been the case. When Congress passed anti-fraud legislation in 2000, the next year SSA misinterpreted provisions in the new law because it did not specifically carve out the exclusion for burial trusts. Therefore, SSA had the power to end the exclusion—and in fact, it did. SSA later realized its mistake and restored the exclusion. However, in the meantime, this hiccup created a wave of chaos for responsible seniors who were wrongly denied access to SSI. This bill will codify the exclusion, so this or future administrations will not even have the possibility of making that mistake again. In doing so, we will not only provide clarity to the administrative agencies, but will also give certainty to SSI enrollees and applicants. They will be ensured that planning ahead to protect their loved ones from the costs associated with death will in no way penalize them when applying for assistance.

We are all aware that Americans are facing difficult times with unacceptably high unemployment and an economy that continues to sag. That is why it is unfair to penalize individuals who are fiscally responsible; rather we should further encourage them to plan ahead. This is not a loophole or a giveaway; this is current policy at SSA, and remember that this exclusion is only for funds or insurance that are absolutely going to be spent on burial costs. They are called ''irrevocable trusts'' because once you put the money aside, you cannot get it back. This bill has negligible revenue effect, because it merely tells the government, firmly, to keep doing what it is already doing.

I should also point to the fact that we are talking about SSI enrollees—individuals who generally do not have a lot of resources. If they are fiscally responsible and plan ahead for their burial and funeral costs, this reduces the likelihood of these costs falling on the obligation of State and local governments.

I know that we want agencies like SSA to be able to use their discretion and be nimble enough to adapt to a changing environment. However, we have gone that route before, and because of the SSA's mistake in reversing the exclusion in 2001, we need to be absolutely clear about the intent of Congress on this policy. It is unconscionable for seniors to have their applications erroneously delayed or denied, and it is incumbent upon us to enact this simple, straightforward, uncontroversial fix.

Americans sacrifice a portion of every paycheck in order to support the programs SSA administers. They do so willingly, knowing that when they retire, or should they become disabled or fall on hard times during old age, programs like SSI will be there for them. This is a promise that we in Congress made to Americans. Enacting this fix is part of keeping that promise.

As a senior member of the Senate Finance Committee, I worked with SSA in developing this language. Many members have expressed support both for this legislation, and for the underlying policy that it codifies. I urge my colleagues to support enactment of this bill, so that we can keep our promise to the Nation's seniors, provide certainty, and reward fiscal responsibility and prudent planning.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 2150

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

SECTION 1. CERTAIN FUNERAL AND BURIAL ARRANGEMENTS NOT CONSIDERED RESOURCES.

(a) IN GENERAL.—Section 1613(d) of the Social Security Act (42 U.S.C. 1382b(d)) is amended—

(1) in paragraph (2)(B), by inserting '', including a trust or arrangement described in paragraph (5)'' after ''irrevocable arrangement''; and

(2) by adding at the end the following:

''(5) If—

''(A) an individual or the individual's spouse enters into an irrevocable contract with a provider of funeral goods and services for a funeral; and

''(B) the individual or the individual's spouse funds the contract by—

''(i) prepaying for the goods and services and the funeral provider places the funds in a trust;

''(ii) establishing an irrevocable trust fully funding the goods and services and the funeral provider is the named beneficiary of the trust, or

''(iii) purchasing a life insurance policy that provides benefits to pay for the goods and services and irrevocably assigning such benefits to—

''(I) the funeral provider; or

''(II) an irrevocable trust fully funding the goods and services and the funeral provider is the named beneficiary of the trust,

then the irrevocable contract and the funding arrangement for the irrevocable contract shall not be considered a resource available to the individual or the individual's spouse.''.

(b) CONFORMING AMENDMENT.—Section 1613(e)(3)(B) of such Act (42 U.S.C. 1382b(e)(3)(B)) is amended by striking ''In the case of an irrevocable trust established by an individual, if there are any circumstances under which payment from the trust'' and inserting ''Except as provided in subsection (d)(5)(B)(ii), if there are any circumstances under which payment from an irrevocable trust established by an individual''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply to payments for supplemental security income benefits under title XVI of the Social Security Act for months beginning on or after the date of enactment of this Act.

By Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin):

S. 2151. A bill to improve information security, and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mr. MCCAIN. Mr. President, I come to the floor today to introduce the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act, also known as the SECURE IT Act. I am joined today by Senator HUTCHISON, Senator CHAMBLISS, Senator GRASSLEY, Senator MURKOWSKI, Senator COATS, Senator BURR, and Senator JOHNSON of Wisconsin. My colleagues and I believe that passage of this act would be a significant step towards improving our Nation's cyber defenses.

It is clear to most policy makers that the Internet has transformed nearly all aspects of our lives by breaking down barriers and increasing information efficiencies. Whether you are a student searching for an article to complete a homework assignment or a fireman trying to remotely determine the landscape of a forest to safely extinguish a fire, the Internet has improved our lives because it has so greatly transformed how and when we are able to access information.

While progress is clear, not a week goes by without fresh media reports of a major compromise of a cyber network in the United States. A recent report by the Government Accountability Office stated that cyber attacks against the United States are up 650 percent over the last 5 years, and according to one leading cybersecurity firm, the annual cost of cyber crime itself is nearly $388 billion. That cost is close to the sum of all of the profits of the top 75 Fortune 500 firms for 2011. My friends, if the top 75 American businesses lost all of their profits in one year, we would be working night and day to solve the problem.

Most of us don't need an analogy like that to appreciate the need to improve the current state of cybersecurity in this country. But the reality is that advancing much needed legislation has been extremely difficult. I will be the first to admit there are honest differences within the cybersecurity debate. However, over the course of the last few years, several cybersecurity solutions have been brought forth that I believe can be advanced and offer insight as to where progress can be achieved. These solutions are not insignificant and their passage would do plenty to improve our country's cybersecurity defenses. I believe that inaction is no longer an option. The stakes are too high and the threat is too real.

The SECURE IT Act is a serious response to the growing cyber threat facing our country. Our bill seeks to utilize the world-class engineers employed by our private sector, not compliance attorneys in billable by the hour law firms. This is why a primary objective of our bill is to enter into a cooperative information sharing relationship with the private sector, rather than an adversarial one rooted in prescriptive Federal regulations used to dictate technological solutions to industry.

The centerpiece of the SECURE IT Act is a legal framework to provide for voluntary information sharing. Our bill provides specific authorities relating to the voluntary sharing of cyber threat information among private entities, between a private entity and a non-federal government agency such as a local government, and between any entity and a pre-existing Federal cybersecurity center. In setting forth our information sharing framework, we do not create any new bureaucracy.

Further, the SECURE IT Act includes no government monitoring, no government take-overs of the Internet, and no government intrusions. There are plenty of laws that deal with those issues—this bill is not one of them. The goal of the information sharing title is to remove the legal hurdles which prevent critical information from being shared with those who need it most.

In drafting the information sharing title of our bill, my colleagues and I were very sensitive to the issue of privacy and we worked very hard to put forth understandable privacy protections. First, we limit the type of information involved in information sharing

to ''cyber threat information'' as it is narrowly defined in the bill. There are no legal protections for entities using, receiving, or sharing information that falls outside that narrow ''cyber threat information'' definition. Second, we include techniques like information anonymizing and specifically state that entities can restrict the further dissemination of shared information. Additionally, after the first year, and then every other year, we will receive reports from the Privacy and Civil Liberties Oversight Board which will tell us how these authorities are being implemented. We take the issue of privacy very seriously.

In addition to information sharing, the SECURE IT Act requires the Federal Government to improve its own cybersecurity by reforming the Federal Information Security Management Act—the law that governs federal networks. These updates are meant to ensure that the Federal Government transitions from paper-based reporting on network security to real-time monitoring—a huge step in federal cybersecurity which will go a long way to improve how the government addresses its own cyber threats. This transition from a checklist approach to continuous monitoring will not happen without an associated cost. However, we believe our approach to this necessary improvement is the most fiscally responsible because we require agencies to meet these requirements by using existing budgets, rather than by authorizing new federal spending.

We are all aware that federal government also plays a critical role in cybersecurity research. The Defense Advanced Research Projects Agency, the Department of Energy laboratories and the National Science Foundation are all world-class leaders in research that is essential to understanding how to best protect our cyber country's infrastructure. This work serves an important purpose and should be a Federal priority even in a time of significant budget constraints. However, the significance of these programs does not provide us with an excuse to authorize new spending or establish new programs. The SECURE IT Act ignores this temptation and does not authorize new spending or programs.

Finally, our cybersecurity bill updates our nation's criminal laws to account for new cyber crimes and assists the Department of Justice to prosecute cyber criminals.

In sum, it is our belief that the provisions included in the SECURE IT Act will dramatically improve cybersecurity in this country. More importantly, the approach taken in the SECURE IT Act has a real chance of being enacted into law this year. This is real progress that will impact nearly all Americans. After all, we are all in this fight together, and as we search for solutions, our first goal should be to move forward together.

Mrs. HUTCHISON. Mr. President, I rise to talk about a bill that was introduced this morning. The bill is the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act, which we refer to as the SECURE IT Act.

This is a very important piece of legislation because we know that cyber attacks are a threat to our country and we need to strengthen our laws to ensure we are protecting our assets, our communication systems, and all of the infrastructure that is run by communications systems.

We are working as a group. Senators MCCAIN, CHAMBLISS, GRASSLEY, MURKOWSKI, COATS, BURR, and JOHNSON are original cosponsors. All of us are the ranking members on the relevant committees that must deal with cybersecurity.

Senator MCCAIN, the lead sponsor, is, of course, the Armed Services ranking member. I am the ranking member of Commerce, Senator CHAMBLISS of Intelligence, Senator GRASSLEY certainly of Judiciary, and Senator MURKOWSKI of Energy.

It is very important that our relevant committees have come together with our ranking members, and we hope very much to gain support from the Democratic side as well on a bill that we think can get through all of Congress and be signed by the President because the parts of our bill that will strengthen our cybersecurity in this country are, I think, accepted by those who have expertise in this area. For instance, our bill will help prevent the spread of cyber attacks from network to network and across the Internet by removing barriers to sharing information about threats, attacks, and strategies for improvement of defenses. We remove these barriers through addressing the antitrust laws that would allow companies that are sharing information not to be threatened with antitrust suits, because this is a security issue, it is not a competitive issue. Secondly, we want to have liability protection for those who disclose cyber threat information with their peers.

These are things that would be in everyone's interest for us to do, and we do need to address them in legislation. The liability and antitrust protections are available to all companies that would share information, not just those that share with the government but when they can talk to each other, to understand each other's systems.

Further, the SECURE IT Act would require that Federal contractors providing electronic communication or cybersecurity services to Federal agencies share cyber threat information related to those contracts. Of course, when they have contracts with the government, that information is going to be very important so we would require the sharing of information about threats that might jeopardize the system's security.

In addition, the government will develop procedures for the timely sharing of classified, declassified, and unclassified information to ensure that information needed to secure networks is fully accessible to trusted parties.

We are concerned that there are other bills out there that will add another new bureaucracy, another layer of regulation that is not necessary and brings in another agency that would overlay the security agencies that already have systems in place. It would also allow the regulatory bodies for certain areas of interest to handle the cybersecurity rather than another overlay of a new department.

I think so many people in our country who are in business feel they are overwhelmed with duplicative regulations and different agencies they have to report to. We want to streamline whom they have to report to and try to use existing structures and existing regulatory authorities to deal with each individual company or industry so that we don't have to give them yet another new bureaucracy that would then have regulations, if they are deemed to be critical infrastructure. That is when it becomes the regulatory threat.

We believe the private sector is more aware of individual security needs and better equipped than the Department of Homeland Security to secure its own networks, working with its own regulators. According to the Office of Management and Budget, the government itself has had great difficulty in preventing attacks on Federal systems. So we do require that the reporting of Federal contractors go to the Federal security agencies, but we don't think the Federal agencies being in charge of everything is necessarily an improvement.

We want to make sure the Federal Information Security Management Act, which is the law, is actually updated so that the new forms of cyber threats are accommodated in FISMA, the Federal Information Security Management Act, and to strengthen that with the updates.

The legislation also updates the Criminal Code to address cyber crimes, strengthening penalties, improving the Department of Justice's ability to prosecute this kind of criminal who would take down whole systems of our government.

Our bill will prioritize cybersecurity research and development so we can harness innovation to protect our country and our private industries from cyber attacks.

I am very pleased that we have been able to introduce this legislation as an alternative to some of the other bills that have come out. I believe that if we can go forward with negotiating, perhaps we can come to an accommodation with the bills that have been introduced with other sponsors. But we don't think the bills that have been introduced address our concerns and we want to ensure that we do not have another big Federal bureaucracy, that we do not overlay the regulators who already have expertise in this area with new regulators whom we have to train

and deal with. We think the defense agencies—the National Security Agency, the Defense Intelligence Agency, the CIA, DHS—all of those with their cybersecurity assets already in place are the better place to put the strength, not reinventing the wheel but better utilizing the systems we already have.

I think it is time for our Senate to address cyber security. I think we have good proposals out there; perhaps we can take the best of those. I think this is the right approach, and Senators MCCAIN, CHAMBLISS, GRASSLEY, and MURKOWSKI were key to drafting this legislation that I think will get the support of all of the stakeholders, as well as the House of Representatives, to actually pass a bill to improve our systems and take it to the President for signature.

Mr. CHAMBLISS. Mr. President, I rise today to speak in support of the Strengthening and Enhancing Cybersecurity by Using Research, Information, and Technology Act of 2012, otherwise known as the SECURE IT Act. This bill provides a strong foundation for Congress to enact what I hope can be a truly bipartisan approach for improving the ability of all Americans to protect themselves against the ever-increasing cybersecurity threat.

This bill was dropped today under the leadership of Senator MCCAIN, Senator HUTCHISON, Senator GRASSLEY, Senator MURKOWSKI, and myself, and I am very pleased to be a part of that group who has worked very hard on this bill for a number of months.

There are a few who dispute the significance of the problem posed by the threat of cyber attacks. The financial harm inflicted by these attacks is now costing Americans billions of dollars each year. Denial-of-service attacks have been shutting down the Internet presence of business and organizations for years. Beyond the economic costs, malicious cyber activity is damaging our national security. Every day, cyber criminals and foreign adversaries steal large amounts of sensitive information from the networks of government and private sector entities. These trends need to be reversed before these malicious activities are measured in terms of lives lost rather than in terms of dollars as we are seeing today.

For years the Senate Intelligence Committee has been following the growing cybersecurity threats. Early on, one of the most common questions asked in the cybersecurity context was, Who is in charge? While this seems like the natural place to start, it is important to understand why this is really not the right question.

First, there is no consensus on who should be in charge. Some have argued it should be the Department of Defense. Some say it should be the Department of Homeland Security. Others think it might be best to start from scratch. All of these options have very obvious drawbacks.

Second, and more important, we have been looking through the wrong end of the telescope in trying to answer this question. Rather than trying to find a governmental entity that should be in charge of cybersecurity, it turns out that the answer is actually much simpler: each and every one of us is in charge of our own cybersecurity. I know some people will scoff at this answer because it is too simplistic for such a complicated problem or they just don't trust us to act in our own best interests. I think they are wrong on both counts.

So, if we—and by ''we,'' I mean all of us who use and rely on computer networks, whether individuals, groups, organizations, corporations, or government agencies—are in charge of our own cybersecurity, the real question then is, What should be done to reduce the threat of malicious cyber activity? I believe the answer to that question is contained in the bill called the SECURE IT Act that we have filed today.

The SECURE IT Act consists of four key areas of common ground identified in various legislative efforts: first, information sharing; second, Federal Information Security Management Act reform; third, enhanced criminal penalties; and fourth, cybersecurity research and development.

We have seen firsthand the positive impact better information sharing can have on our national security. Since the 9/11 terrorist attack, improved information sharing throughout the government and especially within the intelligence community has greatly enhanced our national security. I believe a similar improvement to information sharing in the cyber context will pay huge, long-term dividends in terms of our safety and national security.

Once there is an understanding that information sharing will work best if it empowers the individual rather than a discrete government entity, the move from a regulatory approach to one that encourages voluntary sharing of cyber threat information by removing unintended barriers quickly follows. The information-sharing title of the SECURE IT Act is based on this voluntary approach and on the principle that government cannot and should not solve every problem.

The cosponsors of this bill relied upon a number of principles and practical considerations to develop the information-sharing provisions in this bill.

First, private sector innovation is the engine that drives our economy. Private sector entities have a vested interest in protecting their assets, businesses, and investments. What they often lack is information to help them better protect themselves. Therefore, our information-sharing provision authorizes private sector entities and non-Federal Government agencies to voluntarily disclose cyber threat information to government and private sector entities. The only time cyber threat information must be shared with the government is when it is directly related to a contract between a communications service provider and the government, which ordinarily is a term included in that contract anyway. The only new requirement is that such information will ultimately need to be shared with a cybersecurity center.

Information sharing is and must be a two-way street, but there are no quid pro quos here. Because the government often sees different threat pictures than the private sector, our bill also encourages the government to immediately share more classified, declassified, and unclassified cyber threat information. As one example, consider how improved information sharing might safeguard transportation industry systems. Suppose a commercial airline company detects a virus in their reservation system. The virus is stealing information, including customers' credit card numbers, and sending it to a hacker's server overseas. The airline, after investigating internally, determines where the stolen data is being sent. Under our bill, the airline may share the Internet address that is receiving the stolen credit card information with any other companies, such as other airlines, as well as with the government. With this warning from the first airline, other transportation companies can check their systems to see if any of their data is being sent to the hacker's server. Moreover, using the hacker's Internet address, law enforcement is able to begin an investigation to identify other victims of the same hacker.

The cybersecurity centers will also be able to notify private entities of the nature of this particular threat. In this example, it is unlikely that the airline will ever need to share or release any customer's personally identifiable information.

Second, my cosponsors and I intentionally omitted a critical infrastructure title because we believe a top-down regulatory approach will stifle the voluntary sharing of cyber threat information by the private sector. Consistent with this principle, our information-sharing title does not provide any additional authority to any government entity to impose new regulations on the private sector. In fact, the bill prohibits government agencies from using any shared cyber threat information to regulate the lawful activities of an entity. In short, the bill leaves the existing regulatory regime unchanged.

The real difficulty with trying to regulate in this area is that malicious cyber activities occur in real time and are constantly changing. The bureaucracy-driven regulatory process is simply not nimble enough to keep up with the leading cybersecurity practices. Another disadvantage to a regulatory approach is that it gives hackers insight into existing cybersecurity performance requirements and, as a result, potential vulnerabilities. As industry representatives have told us, this could actually make us less safe, not more safe.

Thirdly, our bill does not create any new bureaucracy to facilitate the sharing of cyber threat information. Rather, it relies upon the existing cybersecurity centers and gives private entities the flexibility to share their cyber threat information with any cyber center. To ensure thorough dissemination within the government, each cybersecurity center is required to pass on to other centers any cyber threat information it receives from an entity. Ultimately, we expect that our current decentralized cybersecurity center structure will be energized by an increase in shared cyber threat information. We also think these centers, with their ongoing relationships with many private entities, provide a more robust and secure environment for information sharing than creating new cybersecurity exchanges or a new national center.

Another advantage of our ''no new regulatory authorities'' and ''no new bureaucracy'' approach is it is also a ''no new spending'' approach. Our bill does not authorize any new spending, which is particularly important given our current economic situation.

Fourth, our bill contains clear and unconditional protection from civil and criminal liability for entities that rely upon the authorities in the information-sharing title. Specifically, a private entity cannot be sued or prosecuted for using lawful countermeasures and cybersecurity systems to defend its networks and identify threats. In addition, neither a private entity nor a Federal Government entity can be sued or prosecuted for using, disclosing, or receiving cyber threat information or for the subsequent action or inaction by an entity to which they gave cyber threat information.

These clear liability protections are necessary to encourage robust information sharing. If they are watered down or made conditional on sharing with the government, private sector lawyers will likely discourage their clients from sharing cyber threat information and, at a minimum, sharing will be delayed while lawyers have to be consulted.

The final practical consideration that governed the drafting of our information-sharing title was to provide sensible safeguards for the protection of personal privacy. We accomplished this in a number of ways.

This information-sharing title is focused on the sharing of only ''cyber threat information.'' It is a key definition in the bill. If you study it carefully, you will see it is limited primarily to information related to malicious cyber activities. There is no authorization or liability protection for using, sharing, or receiving information that falls outside of this definition. Nor can private entities use their cybersecurity systems to get information that falls outside this definition. Moreover, it helps to remember that people engaged in malicious cyber activities are essentially trespassers who have no standing to assert privacy interests.

Besides this relatively narrow definition of ''cyber threat information,'' there is an additional privacy mechanism that limits the collection and disclosure of cyber threat information for the purpose of preventing, investigating, or mitigating threats to information security. In other words, if what you are doing is not for these purposes, then you cannot do it under this bill.

Another way this bill protects privacy is by requiring the government to handle all cyber threat information in a reasonable manner that considers the need to protect privacy and allows the use of anonymizing information.

Since information sharing is voluntary under our bill, private sector entities can take any steps to protect their own privacy interests and the privacy of their customers. Moreover, our bill allows private sector entities to require the recipients of their cyber threat information to seek their consent before further disseminating the information.

Finally, Congress will be able to conduct its oversight since our bill requires an implementation report to Congress within 1 year of enactment, with follow-on reports every 2 years thereafter. These reports will give Congress detailed insight into a number of areas, including the degree to which privacy may be impacted by the provisions in this title.

Now that I have identified the key components and advantages of our approach to information sharing, let me explain why we were compelled to draft this separate bill.

All of the cosponsors of the SECURE IT Act agree with Senators LIEBERMAN and COLLINS and the White House that Congress needs to address the cybersecurity threat. When we attempted to participate in the cyber working groups, it became clear pretty early on that it was going to be difficult to come up with a consensus product.

My experience with working on bipartisan bills such as the Intelligence Authorization Act is that we generally start from scratch and only put in those provisions that are agreed to by both sides. If a provision receives an objection, it is not included, but it is understood it may be an amendment during markup or on the floor. This approach always gives us a great starting point that enjoys the overwhelming support of both sides.

Since the working group process had essentially reached an impasse on the issue of critical infrastructure regulation and how best to promote information sharing, the cosponsors of the SECURE IT Act joined together to develop a bill that would cover ''common ground'' and could serve as a better starting point for negotiations. We have listened to all sides in putting this bill together—government, industry, private groups, cybersecurity experts, and our colleagues on both sides of the aisle in both the Senate and the House. There should be nothing surprising in our bill. Our ranking member group has been telegraphing our priorities for months now.

If we are serious about passing cybersecurity legislation in this Congress—and I hope we are—we should be working together to pass a bill with the support of a large group of Senators far in excess of the 60 we need, as we have done in the past on many major pieces of legislation. I believe the ''common ground'' approach of the SECURE IT Act puts us on a clear path to reaching this goal.

This is important national security legislation. Fortunately, Leaders REID and MCCONNELL have an outstanding record of garnering overwhelming bipartisan support for national security legislation, and I am confident they will seek to do so again. I look forward to continuing these discussions and getting a strong bipartisan bill signed into law.

Ms. MURKOWSKI. Mr. President, I come to the floor today to speak about cybersecurity legislation—legislation we hope will soon be before the Senate.

There is no question—no question at all—that this is a critical issue that should be addressed by this Congress, and I am certain that every Member of this body is concerned that our Nation may be vulnerable to cyber-attacks that could truly have very severe economic and security ramifications. We see stories about cyber-attacks daily—whether they are attacks on individuals, on companies, on government—and I believe it is time for us to take steps to protect ourselves against this emerging threat.

In the coming weeks, the Senate is expected to take up legislation to address this very real problem, and I am hopeful this effort will result in legislation we can all agree is worthy of sending to the President. But right now it appears we are on track to follow an all-or-nothing approach. The problem I see with the bill that is expected to come to the floor—featuring text that was recently released by the Homeland Security and Governmental Affairs Committee—is that it has not gone through regular order and, I fear, amounts to regulatory overreach. If that is our only option here, it will ultimately prevent us from making progress on cybersecurity here in Congress, which I think would be an unfortunate outcome.

Because that outcome is unacceptable, I have introduced an alternative bill this morning, along with a number of ranking member colleagues. I know Senator CHAMBLISS from Georgia was here on the floor earlier, and many of us spoke to it earlier in the day. We call our bill the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012. It has an acronym, of course. It is called SECURE IT for short. The bill follows a commonsense approach to address our ever-increasing cyber threats.

Our bill focuses on four different areas we believe can draw bipartisan

support and result in good public law. Those four areas are: information sharing, FISMA reform—which is intelligence-sharing reform—criminal penalties, as well as additional research.

What the SECURE IT bill does not do is equally important, because it does not simply add new layers of bureaucracy and regulation that will serve little purpose and achieve meager results. The Homeland Security and Governmental Affairs Committee bill would arm the Department of Homeland Security with expansive new authorities to review all sectors of our economy and designate what is termed ''covered critical infrastructure'' for further regulation. What we hear out there from industry is that this amounts to regulation almost for regulation's sake. In the electricity industry's case, this is resulting in duplicative regulation that I am afraid will lead to a ''compliance first'' mentality. Companies will focus on meeting their new Federal requirements and passing a seemingly endless stream of audits, but these heavy-handed statistic requirements from yet one more Federal regulator will not necessarily address the very real threats we face. So again, the concern is we will have industry focused on how do we comply, how do we avoid a bad audit, instead of using their ingenuity and their resources to ensure we stay ahead of any future cyber-attack. We need to be more nimble. We have to have a more nimble approach to dealing with cyber-related threats that are constantly growing and constantly changing. The threat we see today is not necessarily the threat we might anticipate tomorrow, so we have to stay ahead of the game. This is important, and this is where our SECURE IT bill comes in. I think we have simply taken a more pragmatic approach by focusing on the areas where we know we can find some bipartisan support.

One area I think we can all agree on is that the Federal Government needs to form a partnership with the private sector. We share the same goals, that is clear. The goals are to keep our computer systems and our Nation safe from cyber intrusions. We need the private companies to be talking with each other and with the government about the cyber problems they face as well as the potential strategies and the solutions to combat them. To achieve this goal, our legislation encourages the voluntary sharing of much needed information by removing legal barriers to its use and its disclosure. At the same time, we are very careful to safeguard the privacy and prohibit information from being used for competitive advantage.

Our bill also provides necessary updates to the Federal Information Security Management Act. This is the FISMA I spoke to a minute ago. These FISMA reforms require real-time monitoring of Federal systems. It will modernize the way the government manages and mitigates its own cyber risks. And unlike other legislation on this subject, the cyber bill we have introduced today will update criminal statutes to account for cyber activities. Finally, we support advanced cybersecurity research by leveraging existing resources without necessarily spending new Federal dollars. That is very important for us.

This straightforward approach to cybersecurity, I think, can go a long way in tackling the problem. Clearly, our own government agencies here need to be communicating a little bit better with one another. An example of this is that the White House and Department of Homeland Security are staging an exercise next week. All Members have been invited to attend and go through this exercise. It is a mock scenario that will feature a cyber-attack on the Nation's grid. And while I absolutely think this is a useful exercise, and something that is well worthwhile, I do find it quite surprising—quite surprising—that DHS would set up a grid attack scenario and fail to include the grid's primary regulators. These would be the electric reliability organization—what we call NERC—and the Federal Energy Regulatory Commission, or FERC. These are the two regulatory agencies currently in place that provide for that cyber regulation. It is mandated within our grid that these agencies tend to just this issue. So it does make me question if DHS is even aware the electric industry is the only industry already subject to mandatory cyber standards, or that the NERC has the ability to issue time-sensitive alerts to electric utilities in the event of emergency situations. It is kind of hard for me to understand why DHS would proceed with a grid attack simulation and not include the existing governmental entities that already have these safeguards in place. It also begs the question as to whether Congress should provide DHS with such significant and expansive new authorities in the cyber arena.

Before I close, I wish to take a moment to talk about the process behind cybersecurity legislation. While my colleagues and I have highlighted the substantive and procedural problems that are associated with the Homeland Security and Governmental Affairs Committee bill, the majority, and even the press, have attempted to dismiss our arguments as nothing more than partisan stall tactics.

I stand before you to tell you that is simply not true. I want to take action on cyber. I know all of the ranking members who have joined together on this issue want to take action on cyber. We need to do it. I have been calling for action and for legislation since last Congress. We have been working on it in the Energy Committee and have moved out that cyber energy piece. But I do think it is important around this body that there is some meaning to the process; that process really does matter. That is how strong, bipartisan pieces of legislation are enacted. When we forego that process and refuse to do the hard work in the committee—and it is hard. But if we don't do that, we put ourselves on a path to failure with that legislation.

So when we have seven ranking members taking issue with how a bill has been put together, I think we had better pay attention. I think we need to look at whether our process is working.

The SECURE IT bill we introduced today is a strong starting point for us. Some may argue we need to go a little further. But additional layers of bureaucracy and regulations are not the answer at this time. Legislating in the four areas we have highlights—in the information sharing, the FISMA reform, criminal penalties, and research—these are necessary first steps that will make a tremendous amount of difference. If we need to do more in the future, we in Congress can certainly make that determination. But let's not take an all-or-nothing approach to cyber legislation and ultimately end up empty-handed.

I ask my colleagues to take a look at what we have presented today and consider supporting the SECURE IT Act so we can continue to ensure our citizens, our companies, and our country are protected.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 385—CONDEMNING THE GOVERNMENT OF IRAN FOR ITS CONTINUED PERSECUTION, IMPRISONMENT, AND SENTENCING OF YOUCEF NADARKHANI ON THE CHARGE OF APOSTASY

Mr. VITTER (for himself, Mr. RUBIO, Mr. HOEVEN, Mr. DEMINT, Mr. KIRK, Mr. BLUNT, and Mr. HATCH) submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 385

Whereas the United Nations Universal Declaration of Human Rights, adopted at Paris December 10, 1948, and the International Covenant on Civil and Political Rights, adopted at New York December 16, 1966, recognize that every individual has ''the right to freedom of thought, conscience and religion'', which includes the ''freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance'';

Whereas Iran is a member of the United Nations and signatory to both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;

Whereas the United Nations Special Rapporteur on the situation of human rights in Iran has reported that religious minorities, including Nematullahi Sufi Muslims, Sunnis, Baha'is, and Christians, face human rights violations in Iran;

Whereas, in recent years, there has been a significant increase in the number of incidents of authorities in Iran raiding religious services, detaining worshipers and religious leaders, and harassing and threatening members of religious minorities;

Whereas the United Nations Special Rapporteur on the situation of human rights