York (Mr. SCHUMER) was added as a cosponsor of S. 3411, a bill to provide for the adjustment of status for certain Haitian orphans paroled into the United States after the earthquake of January 12, 2010.

S. 3434

At the request of Mr. BINGAMAN, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 3434, a bill to provide for the establishment of a Home Star Retrofit Rebate Program, and for other purposes.

S. 3447

At the request of Mr. AKAKA, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of S. 3447, a bill to amend title 38, United States Code, to improve educational assistance for veterans who served in the Armed Forces after September 11, 2001, and for other purposes.

S. 3461

At the request of Mr. VITTER, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3461, a bill to create a fair and efficient system to resolve claims of victims for economic injury caused by the Deepwater Horizon incident, and to direct the Secretary of the Interior to renegotiate the terms of the lease known as ''Mississippi Canyon 252'' with respect to claims relating to the Deepwater Horizon explosion and oil spill that exceed existing applicable economic liability limitations.

S. 3462

At the request of Mrs. SHAHEEN, the names of the Senator from Oregon (Mr. MERKLEY) and the Senator from Washington (Ms. CANTWELL) were added as cosponsors of S. 3462, a bill to provide subpoena power to the National Commission on the British Petroleum Oil Spill in the Gulf of Mexico, and for other purposes.

S.J. RES. 29

At the request of Mr. MCCONNELL, the name of the Senator from Florida (Mr. LEMIEUX) was added as a cosponsor of S.J. Res. 29, a joint resolution approving the renewal of import restrictions contained in the Burmese Freedom and Democracy Act of 2003.

S. RES. 519

At the request of Mr. DEMINT, the name of the Senator from Idaho (Mr. CRAPO) was added as a cosponsor of S. Res. 519, a resolution expressing the sense of the Senate that the primary safeguard for the well-being and protection of children is the family, and that the primary safeguards for the legal rights of children in the United States are the Constitutions of the United States and the several States, and that, because the use of international treaties to govern policy in the United States on families and children is contrary to principles of self-government and federalism, and that, because the United Nations Convention on the Rights of the Child undermines traditional principles of law in the United States regarding parents and children, the President should not transmit the Convention to the Senate for its advice and consent.

S. RES. 548

At the request of Mr. CORNYN, the name of the Senator from Arizona (Mr. KYL) was added as a cosponsor of S. Res. 548, a resolution to express the sense of the Senate that Israel has an undeniable right to self-defense, and to condemn the recent destabilizing actions by extremists aboard the ship Mavi Marmara.

AMENDMENT NO. 4312

At the request of Mr. VITTER, the names of the Senator from Alabama (Mr. SHELBY) and the Senator from Alaska (Mr. BEGICH) were added as cosponsors of amendment No. 4312 proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

AMENDMENT NO. 4321

At the request of Mr. CASEY, the names of the Senator from Vermont (Mr. LEAHY), the Senator from Hawaii (Mr. AKAKA), the Senator from New Jersey (Mr. MENENDEZ), the Senator from Oregon (Mr. MERKLEY), the Senator from Pennsylvania (Mr. SPECTER), the Senator from Delaware (Mr. KAUFMAN), the Senator from New York (Mr. SCHUMER), the Senator from Illinois (Mr. DURBIN) and the Senator from Maryland (Ms. MIKULSKI) were added as cosponsors of amendment No. 4321 intended to be proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

AMENDMENT NO. 4324

At the request of Mr. WHITEHOUSE, the names of the Senator from Massachusetts (Mr. BROWN), the Senator from Vermont (Mr. LEAHY) and the Senator from Missouri (Mrs. MCCASKILL) were added as cosponsors of amendment No. 4324 intended to be proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

AMENDMENT NO. 4327

At the request of Ms. MURKOWSKI, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of amendment No. 4327 intended to be proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

AMENDMENT NO. 4332

At the request of Mr. KOHL, the name of the Senator from Minnesota (Mr. FRANKEN) was added as a cosponsor of amendment No. 4332 intended to be proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

AMENDMENT NO. 4333

At the request of Mr. THUNE, the name of the Senator from Georgia (Mr. ISAKSON) was added as a cosponsor of amendment No. 4333 intended to be proposed to H.R. 4213, a bill to amend the Internal Revenue Code of 1986 to extend certain expiring provisions, and for other purposes.

At the request of Mr. MCCONNELL, his name was added as a cosponsor of amendment No. 4333 intended to be proposed to H.R. 4213, supra.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mrs. HAGAN (for herself, Mr. CASEY, and Ms. LANDRIEU):

3479. A bill to authorize the Secretary of Health and Human Services, acting through the Director of the Centers for Disease Control and Prevention, to establish and implement a birth defects prevention, risk reduction, and public awareness program; to the Committee on Health, Education, Labor, and Pensions.

Mrs. HAGAN. Mr. President, today I am proud to introduce the Birth Defects Prevention, Risk Reduction, and Awareness Act. This bill would ensure that women of childbearing age and health care professionals have access to clinical and evidence based information about the risks and benefits of drug, chemical, and nutritional exposures during pregnancy and while a woman is breastfeeding.

Women who are pregnant or breastfeeding and taking medication for chronic diseases such as asthma, hypertension, and epilepsy often have questions about the risks and benefits. Most pregnant women, as we witnessed last year, really want to know what the science indicates on whether they should get vaccinated against H1N1 or the seasonal flu.

Oftentimes, women will seek answers to these important questions from an established pregnancy and breastfeeding information service. In fact, each year over 70,000 women and health care providers contact these information services across the country. These information services provide valuable information that empowers women. In fact, one study indicated that 78 percent of women who were considering terminating otherwise wanted pregnancies due to fears about exposing their fetus to a medication changed their mind after receiving appropriate counseling from a teratology information service.

It is not just women who use these services; health care providers, including physicians and pharmacists, also utilize these pregnancy and breastfeeding information services. A 2009 study found that over 90 percent of physicians who use these services indicated that the service provides high quality information that has a significant impact on clinical care.

In North Carolina, we have the North Carolina Pregnancy Exposure Riskline, run out of Mission Health System in Asheville. The North Carolina Pregnancy Exposure Riskline fields calls from a variety of constituents, including health care providers, pregnant

women, preconception women, potential adoptive parents, and others. Each year, trained genetic counselors answer questions from over 300 callers, who want information on the impact of maternal exposures during pregnancy and while breastfeeding.

The North Carolina Pregnancy Exposure Riskline provides detailed, factual information to callers on the current available data, and makes referrals to pregnancy registries that are continuing to gather information so that researchers and health care providers can have the best information for future women. If needed and requested, counselors will refer women to pregnancy resources such as substances treatment facilities or the NC Family Health Resource line, which has led North Carolina in information campaigns on the benefits of folic acid and ''Back to Sleep.''

The North Carolina Pregnancy Exposure Riskline also supports the North Carolina Teratology Information Specialists program to provide outreach and education about fetal alcohol syndrome.

Although this is an invaluable service for many women, physicians, and other health care providers, pregnancy and breastfeeding information services across the country have been forced to close due to insufficient funding.

The bill I am introducing today would require the Secretary of Health and Human Services, through the Centers for Disease Control and Prevention, to implement a birth defects prevention and public awareness grant program. Specifically, CDC would initiate a national media campaign to increase awareness among health care providers and at risk populations about pregnancy and breast feeding information services. Experienced organizations would be eligible to apply for grants: to provide information; and to conduct surveillance and research of pregnancy exposures that may cause birth defects, prematurity or other adverse pregnancy outcomes, and maternal exposures that may cause harm to a breast-fed infant.

I am so pleased that the American Academy of Pediatrics, the American Congress of Obstetricians and Gynecologists, the March of Dimes, the Organization of Teratology Information Specialists, and the American Academy of Asthma & Immunology are in support of this worthwhile bill.

I urge my other colleagues to join me in supporting this important bill to provide valuable information about maternal exposures during pregnancy and while breastfeeding.

By Mr. LIEBERMAN (for himself, Ms. COLLINS, and Mr. CARPER):

S. 3480. A bill to amend the Homeland Seeurity Act of 2002 And other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States; to the Committee on Homeland Security and Governmental Affairs.

Mr. LIEBERMAN. Mr. President, I rise today to introduce the Protecting Cyberspace as a National Asset Act of 2010, which I believe would help secure the Nation's cyber networks against attack.

The Internet may have started out as a communications oddity some 40 years ago but it is now a necessity of modern life and, sadly, one that is under constant attack. Today, Senators COLLINS, CARPER, and I are introducing legislation which we believe would help secure the most critical cyber networks and therefore all Americans.

For all of its ''user-friendly'' allure, the Internet can also be a dangerous place with electronic pipelines that run directly into everything from our personal bank accounts to key infrastructure to government and industrial secrets. Our economic security, national security and public safety are now all at risk from new kinds of enemies—cyber-warriors, cyber-spies, cyberterrorists and cyber-criminals. That risk may be as serious to our homeland security as anything we face today.

Computer networks at the Departments of Defense are being probed hundreds of thousands of times a day, and networks at the Departments of State, Homeland Security and Commerce, as well as NASA and the National Defense University, have all suffered ''major intrusions by unknown foreign entities,'' according to reports.

Key networks that control vital infrastructure, like the electric grid, have been probed, possibly giving our enemies information that could be used to plunge us into darkness at the press of a button from across an ocean. Banks have had millions and millions of dollars stolen from accounts by cyber-bandits who have never been anywhere near the banks themselves.

In a report by McAfee—a computer security company, about 54 percent of the executives of critical infrastructure companies surveyed said their companies had been the victims of denial of service attacks or network infiltration by organized crime groups, terrorists, and other nation-states. The downtime to recover from these attacks can cost $6 million to $8 million a day.

Our present efforts at securing these vital but sprawling government and private sector networks have been disjointed, understaffed and underfinanced. We have not operated with the sense of urgency that is necessary to protect Americans' cyberspace, which the President has correctly described as a ''strategic national asset.''

Our bill would bring these disjointed efforts together so that the federal government and the private sector can coordinate their activities and work off the same playbook.

While President Obama's creation of a cyber-security coordinator inside the White House was a step in the right direction, we need to make that position permanent, transparent and accountable to Congress and the American people.

So, our proposal would create a Senate-confirmed White House cyber-security coordinator whose job would be to lead all federal cyber-security efforts; develop a national strategy—that incorporates all elements of cyberspace policy, including military, law enforcement, intelligence, and diplomatic; give policy advice to the President; and resolve interagency disputes.

The Director of the Office of Cyberspace Policy would oversee all related federal cyberspace activities to ensure efficiency and coordination and would report regularly to Congress to ensure transparency and oversight.

Our legislation also would create a National Center for Cybersecurity an Communications, NCCC, within the Department of Homeland Security, DHS, to elevate and strengthen the Department's cyber security capabilities and authorities. The NCCC would be run by a Senate-confirmed Director who would have the authority and resources to work with the rest of the Federal Government to protect public and private sector cyber networks.

DHS has shown that vulnerabilities in key private sector networks—like utilities and communications systems—could bring our economy to its knees if attacked or commandeered by a foreign power or cyber-terrorists. But other than pointing out a vulnerability, DHS has lacked the power to do anything about it. Our legislation would give DHS the authority to ensure that our nation's most critical infrastructure is protected from cyber attack.

Defense of our cyber networks will only be successful if industry and government work together, so this legislation sets up a collaborative process where the best ideas of the private sector and the government can be used to meet a baseline set of security requirements that DHS would oversee.

Specifically, the NCCC would work with the private sector to establish risk-based security requirements that strengthen the cyber security for the nation's most critical infrastructure, such as vital components of the electric grid, telecommunications networks, and financial sector that, if disrupted, would result in a national or regional catastrophe. Owners and operators of critical infrastructure covered under the act could choose which security measures to implement to meet these risk-based performance requirements. The act would provide some liability protections to owners/operators who demonstrate compliance with the new risk-based security requirements.

Covered critical infrastructure must also report significant breaches to the NCCC to ensure the federal government has a complete picture of the security of these networks. In return, the NCCC would share information, including threat analysis, with owners and operators regarding risks to their networks. The NCCC would also produce and

share useful warning, analysis, and threat information with other Federal agencies, State and local governments, and international partners.

To increase security across the private sector more broadly, the NCCC would collaborate with the private sector to develop best practices for cyber security. By promoting best practices and providing voluntary technical assistance as resources permit, the NCCC would help improve cyber security across the Nation. Information the private sector shares with the NCCC would be protected from public disclosure, and private sector owners and operators may obtain security clearances to access information necessary to protect the IT networks the American people depend upon.

Thanks to great work by Senator CARPER, our legislation would update the Federal Information Security Management Act—or FISMA—to require continuous monitoring and protection of our federal networks and do away with the paper-based reporting system that currently exists. The act also would codify and strengthen DHS authorities to establish0 complete situational awareness for Federal networks and develop tools to improve resilience of Federal Government systems and networks.

In the event of an attack—or threat of an attack—that could have catastrophic consequences to our economy, national security or public safety, our bill would give the President the authority to impose emergency measures on a select group of the most critical infrastructure to preserve their cyber networks and assets and protect our country and the American people. These emergency measures would automatically expire within 30 days unless the President ordered an extension.

These measures would be developed in consultation with the private sector and would apply if the President has credible evidence a cyber vulnerability is being exploited or is about to be exploited. If possible, the President must notify Congress in advance about the threat and the emergency measures that would be taken to mitigate it. Any emergency measures imposed must be the least disruptive necessary to respond to the threat. The bill does not authorize any new surveillance authorities, or permit the government to ''take over'' private networks.

Of course, DHS would need a lot of talented people to accomplish these missions, and our bill gives it the flexibility to recruit, hire, and retain the experts it would need to be successful. Our bill would require the Office of Personal Management to reform the way cyber security personnel are recruited, hired, and trained and would provide DHS with temporary hiring and pay flexibilities to assist in the quick establishment of the NCCC.

Finally, our legislation would require the Federal Government to develop and implement a strategy to ensure that almost $80 billion of the information technology products and services it purchases each year are secure and do not provide our adversaries with a backdoor into our networks.

More specifically, the act would require development of a comprehensive supply chain risk management strategy to address risks and threats to the information technology products and services the federal government relies upon. This strategy would allow agencies to make informed decisions when purchasing IT products and services. This provision would be implemented through the Federal Acquisition Regulation, requiring contracting officers to consider the security risks inherent in agency IT procurements. The value of this approach is that once security features are developed to protect federal networks, private sector customers may be able to purchase that same level of security in the products they buy.

The need for this legislation is both obvious and urgent.

A report by the bipartisan Center for Strategic and International Studies, CSIS, concluded that ''we face a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals and others, and losing this struggle would wreak serious damage on the economic health and national security of the United States.''

Given these stakes, Senators COLLINS, CARPER, and I are confident our colleagues will join with us and pass the ''Protecting Cyberspace as a National Asset Act'' in the 110th Congress.

Ms. COLLINS. Mr. President, I rise to join Senators LIEBERMAN and CARPER in introducing the Protecting Cyberspace as a National Asset Act of 2010. This vital legislation would fortify the government's efforts to safeguard America's cyber networks from attack. It would build a public/private partnership to promote national cyber security priorities. It would strengthen the government's ability to set, monitor compliance with, and enforce standards and policies for securing Federal civilian systems and the sensitive information they contain.

The marriage of increasingly robust computer technology to expanding and nearly instantaneous global telecommunications networks is a truly seismic event in human history. This information revolution touches everything, from personal relationships and entertainment to commerce, scientific research, and the most sensitive national security information. Cyberspace is a place of great, even unparalleled, power.

But, to tweak the familiar saying, with great power comes great vulnerability. Cyberspace is under increasing assault on all fronts: cyber vandalism, cyber crime, cyber sabotage, and cyber espionage. Across the world at this moment, computer networks are being hacked, probed, and infiltrated relentlessly. The purpose of these cyber exploits ranges from simple mischief and massive theft to societal mayhem and geopolitical advantage.

In February, Dennis Blair, the former Director of National Intelligence, gave this chilling assessment before the Senate Select Committee on Intelligence:

''Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication. While both the threats and technologies associated with cyberspace are dynamic, the existing balance in network technology favors malicious actors, and is likely to continue to do so for the foreseeable future.''

Consider these sobering facts:

Cyber crime costs our national economy nearly $8 billion annually.

Hackers can operate in relative safety and anonymity from a laptop or desktop anywhere in the world. The expanding capabilities of wireless handheld devices strengthen this cloak of cyber invisibility.

As our national and global economies become ever more intertwined, cyber terrorists have greater potential to attack high-value targets. From anywhere in the world, they could disrupt telecommunications systems, shut down electric power grids, or freeze financial markets. With sufficient know-how and a few keystrokes, they could cause billions of dollars in damage and put thousands of lives in jeopardy.

As the hackers' techniques advance, the number of hacking attempts is exploding. Just this March, the Senate's Sergeant at Arms reported that the computer systems of Congress and Executive Branch agencies now are under cyber attack an average of 1.8 billion times per month.

Recent examples of cyber attacks are myriad and disturbing:

Press reports a year ago stated that China and Russia had penetrated the computer systems of America's electrical grid. The hackers allegedly left behind malicious hidden software that could be activated later to disrupt the grid during a war or other national crisis.

At about the same time, we learned that, beginning in 2007 and continuing well into 2008, hackers repeatedly broke into the computer systems of the Pentagon's $300-billion Joint Strike Fighter project. They stole crucial information about the Defense Department's costliest weapons program ever.

In 2007, the country of Estonia was attacked in cyberspace. A 3-week onslaught of botnets overwhelmed the computer systems of the nation's parliament, government ministries, banks, telecommunications networks, and news organizations. This attack on Estonia is a wake-up call that has yet to be sufficiently heeded.

The private sector is also under attack. In January, Google announced that attacks originating in China had targeted its systems as well as the networks of more than 30 other companies. The attacks on Google sought to access the email accounts of Chinese

human rights activists. For the other companies, lucrative information, such as critical corporate data and software source codes, were targeted.

Last year, cyber thieves secretly implanted circuitry into keypads sold to British supermarkets, which were then used to steal account information and PIN numbers. This same tactic was used against a large supermarket chain in Maine, compromising more than 4 million credit cards.

Nor are small businesses immune. Last summer, a small Maine construction firm found that cyber crooks had stolen nearly $600,000 through an elaborate scheme involving dozens of coconspirators throughout the United States.

These attacks, and the hundreds like them that are occurring at any given time whether on our government or private sector systems, have ushered us into a new age of cyber crime and, indeed, cyber warfare. They underscore the high priority we must give to the security of our information technology systems.

The terrorist attacks of September 11, 2001, exposed the vulnerability of our nation to catastrophic attacks. Since that terrible day, we have done much to protect potential targets such as ports, chemical facilities, transportation systems, water supplies, government buildings, and other vital assets. We cannot afford to wait for a ''cyber 9/11'' before our government finally realizes the importance of protecting our digital resources, limiting our vulnerabilities, and mitigating the consequences of penetrations of our networks.

Chairman LIEBERMAN and I have held a number of hearings on cyber security in the Senate Homeland Security and Governmental Affairs Committee. Senator CARPER has been similarly active, particularly on exploring modifications to the Federal Information Security Management Act that are designed to enhance protections of Federal networks and information.

From our examinations of this issue, we know that there are threats to and vulnerabilities in our cyber networks. We also know that the tactics used to exploit these vulnerabilities are constantly evolving and growing increasingly dangerous. Now, it is time to take action. A strong and sustained Federal effort to promote cyber security is a key component of effective deterrence.

For too long, our approach to cyber security has been disjointed and uncoordinated. This cannot continue. The United States requires a comprehensive cyber security strategy backed by aggressive implementation of effective security measures. There must be strong coordination among law enforcement, intelligence agencies, the military, and the private owners and operators of critical infrastructure.

This bill would establish the essential point of coordination. The Office of Cyberspace Policy in the Executive Office of the President would be run by a Senate-confirmed Director who would advise the President on all cyber security matters. The Director would lead and harmonize Federal efforts to secure cyberspace and would develop a national strategy that incorporates all elements of cyber security policy, including military, law enforcement, intelligence, and diplomacy. The Director would oversee all Federal activities related to the national strategy to ensure efficiency and coordination. The Director would report regularly to Congress to ensure transparency and oversight.

To be clear, the White House official would not be another unaccountable czar. The Cyber Director would be a Senate-confirmed position and thus would testify before Congress. The important responsibilities given to the Director of the Office of Cyberspace Policy related to cybersecurity are similar to the responsibilities of the current Director of the Office of Science and Technology Policy.

The Cyber Director would advise the President and coordinate efforts across the Executive Branch to protect and improve our cybersecurity posture and communications networks. By working with a strong operational and tactical partner at the Department of Homeland Security, the Director would help improve the security of Federal and private sector networks.

This strong DHS partner would be the National Center for Cybersecurity and Communications, or Cyber Center. It would be located within the Department of Homeland Security to elevate and strengthen the Department's cyber security capabilities and authorities. This Center also would be led by a Senate-confirmed Director.

The Cyber Center, anchored at DHS, with a strong and empowered leader, will close the coordination gaps that currently exist in our disjointed federal cyber security efforts. For day-to-day operations, the Center would use the resources of DHS, and the Center Director would report directly to the Secretary of Homeland Security. On interagency matters related to the security of federal networks, the Director would regularly advise the President—a relationship similar to the Director of the NCTC on counterterrorism matters or the Chairman of the Joint Chiefs of Staff on military issues. These dual relationships would give the Center Director sufficient rank and stature to interact effectively with the heads of other departments and agencies, and with the private sector.

Congress has dealt with complex challenges involving the need for interagency coordination in the past with a similar construct. We have established strong leaders with supporting organizational structures to coordinate and implement action across agencies, while recognizing and respecting disparate agency missions.

The establishment of the National Counterterrorism Center within the Office of the Director of National Intelligence is a prime example of a successful reorganization that fused the missions of multiple agencies. The Director of NCTC is responsible for the strategic planning of joint counterterrorism operations, and in this role reports to the President. When implementing the information analysis, integration, and sharing mission of the Center, the Director reports to the Director of National Intelligence. These dual roles provide access to the President on strategic, interagency matters, yet provide NCTC with the structural support and resources of the office of the DNI to complete the day-to-day work of the NCTC. The DHS Cyber Center would replicate this successful model for cyber security.

As we have seen repeatedly, from the financial crisis to the environmental catastrophe in the Gulf of Mexico, what happens in the private sector does not always affect just the private sector. The ramifications for government and for the taxpayers often are enormous.

This bill would establish a public/private partnership to improve cyber security. Working collaboratively with the private sector, the Center would produce and share useful warning, analysis, and threat information with the private sector, other Federal agencies, international partners, and state and local governments. By developing and promoting best practices and providing voluntary technical assistance to the private sector, the Center would improve cyber security across the nation. Best practices developed by the Center would be based on collaboration and information sharing with the private sector. Information shared with the Center by the private sector would be protected.

With respect to the owners and operators of our most critical systems and assets, the bill would mandate compliance with certain risk-based performance requirements to close security gaps. These requirements would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted.

This approach would be similar to the current model that DHS employs with the chemical industry. Rather than setting specific standards, DHS would employ a risk-based approach to evaluating cyber vulnerabilities, and the owners and operators of covered critical infrastructure would develop a plan for protecting those vulnerabilities and mitigating the consequences of an attack.

These owners and operators would be able to choose which security measures to implement to meet applicable risk-based performance requirements. The bill does not authorize any new surveillance authorities or permit the government to ''take over'' private networks. This model would allow for continued

innovation and dynamism that are fundamental to the success of the IT sector.

The bill would provide limited liability protections to the owners and operators of covered critical infrastructure that comply with the new risk-based performance requirements. Covered critical infrastructure also would be required to report certain significant breaches affecting vital system functions to the center. These reports would help ensure that the Federal Government has comprehensive awareness of the security risks facing these critical networks.

If a cyber attack is imminent or occurring, the bill would provide a responsible framework, developed in coordination with the private sector, for the President to authorize emergency measures to protect the Nation's most critical infrastructure. The President would be required to notify Congress in advance of the declaration of a national cyber emergency, or as soon thereafter as possible. This notice would include the nature of the threat, the reason existing protective measures are insufficient to respond to the threat, and the emergency actions necessary to mitigate the threat. The emergency measures would be limited in duration and scope.

Any emergency actions directed by the President during the 30-day period covered by the declaration must be the least disruptive means feasible to respond to the threat. Liability protections would apply to owners and operators required to implement these measures, and if other mitigation options were available, owners and operators could propose those alternative measures to the Director and, once approved, implement those in lieu of the mandatory emergency measures.

The center also would share information, including threat analysis, with owners and operators of critical infrastructure regarding risks affecting the security of their sectors. The center would work with sector-specific agencies and other Federal agencies with existing regulatory authority to avoid duplication of requirements, to use existing expertise, and to ensure government resources are employed in the most efficient and effective manner.

With regard to Federal networks, the Federal Information Security Management Act—known as FISMA—gives the Office of Management and Budget broad authority to oversee agency information security measures. In practice, however, FISMA is frequently criticized as a ''paperwork exercise'' that offers little real security and leads to a disjointed cyber security regime in which each Federal agency haphazardly implements its own security measures.

The bill we introduce today would transform FISMA from paper-based to real-time responses. It would codify and strengthen DHS authorities to establish complete situational awareness for Federal networks and develop tools to improve resilience of Federal Government systems and networks.

The legislation also would take advantage of the Federal Government's massive purchasing power to help bring heightened cyber security standards to the marketplace. Specifically, the Director of the Center would be charged with developing a supply chain risk management strategy applicable to Federal procurements. This strategy would emphasize the security of information systems from development to acquisition and throughout their operational life cycle.

While the Director should not be responsible for micromanaging individual procurements or directing investments, we have seen far too often that security is not a primary concern when agencies procure their IT systems. Recommending security investments to OMB and providing strategic guidance on security enhancements early in the development and acquisition process will help ''bake in'' security. Cyber security can no longer be an afterthought in our government agencies.

These improvements in Federal acquisition policy should have beneficial ripple effects in the larger commercial market. As a large customer, the Federal Government can contract with companies to innovate and improve the security of their IT services and products. With the Government's vast purchasing power, these innovations can establish new security baselines for services and products offered to the private sector and the general public.

Finally, the legislation would direct the Office of Personnel Management to reform the way cyber security personnel are recruited, hired, and trained to ensure that the Federal Government and the private sector have the talent necessary to lead this national effort and protect its own networks. The bill would also provide DHS with temporary hiring and pay flexibilities to assist in the establishment of the center.

Some have suggested that this effort can be led from the White House alone—why create a new center at DHS and two Senate-confirmed Director positions? One of the great lessons of 9/11 is that true security demands aggressive oversight, expert evaluation, and thorough testing of systems. There must be constant, real-time monitoring of security and analysis of threats. This task requires much more than a cyber czar. It requires strong civilian counterparts to the Secretary of Defense and the Director of National Intelligence. These Directors, at the White House and at DHS, would serve as those counterparts.

The National Security Agency and other intelligence agencies possess enormous skills and resources, but privacy and civil liberties demands preclude these agencies from shouldering a leadership role in the security of our civilian information technology systems. The intelligence community must play a critical part in providing threat information, but it cannot lead the cyber security effort.

We are all acutely aware that there are those who seek to do harm to this country and to our people. If hackers can nearly bring Estonia to its knees through cyber attacks, infiltrate our military's most closely-guarded project, and, in the case of Google, hack the computers owned and operated by some of the world's most successful computer experts, we must assume even more spectacular and potentially devastating attacks lie ahead.

We must be ready. It is vitally important that we build a strong public-private partnership to protect cyberspace. It is a vital engine of our economy, our government, our country and our future. I urge my colleagues to support this crucial legislation.

By Mr. CARDIN:

S. 3481. A bill to amend the Federal Water Pollution Control Act to clarify Federal responsibility for stormwater pollution; to the Committee on Environment and Public Works.

Mr. CARDIN. Mr. President, in recent weeks the issue of polluted stormwater runoff from federal properties has again gained significant attention. I continue to have grave concerns about the failure of the Federal Government to pay localities for reasonable costs associated with the control and abatement of pollution that is originating on its properties. At stake is a fundamental issue of equity: polluters should be financially responsible for the pollution that they cause. That includes the Federal Government.

Today I am introducing legislation that makes it clear. Uncle Sam must pay his bills just like every other American.

Annually hundreds of thousands of pounds of pollutants wash off the hardened surfaces in urban areas and into local rivers and streams, threatening the health of our citizens and causing significant environmental degradation. A one-acre parking lot produces about 16 times the volume of runoff that comes from a one-acre meadow. These pollutants include heavy metals, nitrogen and phosphorous, oil and grease, pesticides, bacteria, including deadly e. coli, sediment, toxic chemicals, and debris. Indeed, stormwater runoff is the largest source sector for many imperiled bodies of water across the country. According to the Environmental Protection Agency, stormwater pollution affects all types of water bodies including in order of severity; ocean shoreline, estuaries such as the Chesapeake Bay, Great Lakes shorelines, lakes and rivers. Degraded aquatic habitats are found everywhere that stormwater enters local waterways.

On October 5, 2009, President Obama issued a Federal Executive order on sustainability which set goals for Federal agencies and focused on making improvements in their environmental, energy and economic performance.

Among other requirements, the order specifically requires the implementation of the stormwater provisions of the Energy Independence and Security Act of 2007, section 438.

I am the author of that provision, which requires the Federal Government to maintain the predevelopment hydrology ''to the maximum extent practicable'' of all new building sites or major renovations. This requirement echoed the provision in the President's Chesapeake Bay Protection and Restoration Executive Order issued on May 12, 2009. In the final Strategy for Protecting and Restoring the Chesapeake Bay Watershed, issued on the one-year anniversary of the Executive Order, each Federal agency is being called upon to implement ''the stormwater requirements for new development and redevelopment in Section 438 of the Energy Independence and Security Act. . .'' (pp. 33–34). These parallel Federal stormwater management requirements are explicit recognition of the importance of controlling and managing stormwater pollution from Federal properties.

As EPA requires more communities to address stormwater pollution through Clean Water Act required Municipal Separate Storm Sewer System permits, these communities are responding with a variety of fee-based management systems that will allow them to mitigate, manage and prevent this type of pollution.

The EPA requires National Pollution Discharge Elimination Permits for large communities. The President has issued two Executive Orders that directly note the need to address this type of pollution ''to the maximum extent practicable.'' Clearly, these actions demonstrate that the administration recognizes the importance of dealing adequately with stormwater pollution.

I believe that this administration recognizes its responsibility to manage the stormwater pollution that comes off Federal properties. But that responsibility needs to translate into payments to the local governments that are forced to deal with this pollution. That commitment needs to be more than an Executive order. Adopting the legislation that I am introducing today will remove all ambiguity about the responsibility of the Federal Government to pay these normal and customary stormwater fees.

This is a matter of basic equity. I call upon all of my colleagues to join me in supporting this simple legislative remedy.

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

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

S. 3481

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

SECTION 1. FEDERAL RESPONSIBILITY FOR STORMWATER POLLUTION.

Section 313 of the Federal Water Pollution Control Act (33 U.S.C. 1323) is amended by adding at the end the following:

''(c) FEDERAL RESPONSIBILITY FOR STORMWATER POLLUTION.—Reasonable service charges described in subsection (a) include reasonable fees or assessments made for the purpose of stormwater management in the same manner and to the same extent as any nongovernmental entity.

''(d) NO TREATMENT AS TAX OR LEVY.—A fee or assessment described in this section—

''(1) shall not be considered to be a tax or other levy subject to an assertion of sovereign immunity; and

''(2) may be paid using appropriated funds.''.

By Mr. REID:

S. 3482. A bill to provide for the development of solar pilot project areas on public land in Lincoln County, Nevada; to the Committee on Energy and Natural Resources.

Mr. REID. Mr. President, today I rise to introduce the American Solar Energy Pilot Leasing Act of 2010. Solar energy development is a critical factor in creating jobs and making the United States energy independent. This legislation will provide a pilot program for the Department of the Interior to develop a solar leasing program in Nevada.

The Secretary of the Interior, though the Bureau of Land Management, BLM, is currently developing a west wide solar energy program based on existing laws and regulations. The BLM, however, does not currently have the legal authority to lease public lands for solar development. This bill will establish, in Lincoln County, the first Federal solar leasing program in the U.S., which will serve as a pilot project for the Department of the Interior in order to guide development of solar leasing throughout the west in the years to come.

The American Solar Energy Pilot Leasing Act designates two solar development zones in Lincoln County for commercial solar energy development. The 10,945 acre Dry Lake zone and the 2,845 acre Delamar Valley zone are within high solar potential areas identified by the BLM and were selected by Lincoln County based on extensive public input. Since the solar zones border the Southwest Intertie Project, SWIP, transmission corridor, these projects will create the opportunity for southern Nevada and California to tap directly into Lincoln County's abundant renewable power resources.

Our bill directs the agency to consult with the County and local stakeholders before offering both parcels for lease not more than 60 days after the bill becomes law. In order to ensure efficient and wise development throughout the west, the BLM is also directed to establish diligent development requirements to ensure leased areas are efficiently developed and to promulgate regulations to guide development of the burgeoning solar leasing program.

The act directs the BLM to set a royalty rate at a level that will encourage efficient production of solar energy and ensure a fair return to the public for the necessary development of the public lands. As part of this program, the BLM is given the flexibility to charge a lower royalty, or even no royalty, for up to five years after energy generation begins as an incentive to promote the maximum generation of solar energy.

Royalties and fees from these solar leasing pilot projects will be disbursed into four accounts. Thirty-five percent will be deposited into the Renewable Energy Mitigation Fish and Wildlife Fund—established by this act to protect and restore wildlife and their habitat and to implement the Land and Water Conservation Fund in Nevada. The State of Nevada and Lincoln County will each receive 25 percent of the collected royalties and fees. The last 15 percent will be directed to the BLM to fund renewable energy permit processing over the next 10 years. At the end of that 10-year period, this 15 percent will be directed to the Renewable Energy Mitigation Fish and Wildlife Fund, in addition to the 35 percent initially set aside for this account.

As you know, I have been a longtime champion for the development of clean, renewable energy resources. Nevada has unparalleled potential for solar energy development and is poised to lead our Nation in clean energy development and innovation. This is a significant step toward moving our country away from dirty fossil fuels and creating a new job market in the west. The model established by this legislation will also reinvest a responsible portion of the royalties and fees from solar energy development into the states and rural communities whose land is being used to power our Nation.

I would like to thank Lincoln County and a great number of sportsmen, ranchers, and conservationists who have helped us shape this legislation. I am pleased to bring this bill to the committee and I look forward to working with Chairman BINGAMAN, Ranking Member MURKOWSKI and the other distinguished members to move this bill through the legislative process.

Mr. President, I ask for 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. 3482

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 ''American Solar Energy Pilot Leasing Act of 2010''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COUNTY.—The term ''County'' means Lincoln County, Nevada.

(2) FEDERAL LAND.—The term ''Federal land'' means any of the Federal land in the State under the administrative jurisdiction of the Bureau of Land Management that is identified as a ''solar development zone'' on the maps.

(3) FUND.—The term ''Fund'' means the Renewable Energy Mitigation and Fish and Wildlife Fund established by section 3(d)(5)(A).

(4) MAP.—The term ''map'' means each of—

(A) the map entitled ''Dry Lake Valley Solar Development Zone'' and dated May 25, 2010; and

(B) the map entitled ''Delamar Valley Solar Development Zone'' and dated May 25, 2010.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Interior, acting through the Director of the Bureau of Land Management.

(6) STATE.—The term ''State'' means the State of Nevada.

SEC. 3. DEVELOPMENT OF SOLAR PILOT PROJECT AREAS ON PUBLIC LAND IN LINCOLN COUNTY, NEVADA.

(a) DESIGNATION.—In accordance with sections 201 and 202 of the Federal Land Policy and Management Act of 1976 (43 U.S.C. 1711, 1712) and subject to valid existing rights, the Secretary shall designate the Federal land as a solar pilot project area.

(b) APPLICABLE LAW.—The designation of the solar pilot project area under subsection (a) shall be subject to the requirements of—

(1) this Act;

(2) the Federal Land Policy and Management Act of 1976 (43 U.S.C. 1701 et seq.); and

(3) any other applicable law (including regulations).

(c) SOLAR LEASE SALES.—

(1) IN GENERAL.—The Secretary shall conduct lease sales and issue leases for commercial solar energy development on the Federal land, in accordance with this subsection.

(2) DEADLINE FOR LEASE SALES.—Not later than 60 days after the date of enactment of this Act, the Secretary, after consulting with affected governments and other stakeholders, shall conduct lease sales for the Federal land.

(3) EASEMENTS, SPECIAL-USE PERMITS, AND RIGHTS-OF-WAY.—Except for the temporary placement and operation of testing or data collection devices, as the Secretary determines to be appropriate, and the rights-of-way granted under section 301(b)(1) of the Lincoln County Conservation, Recreation, and Development Act of 2004 (Public Law 108–424; 118 Stat. 2413) and BLM Case File N–78803, no new easements, special-use permits, or rights-of-way shall be allowed on the Federal land during the period beginning on the date of enactment of this Act and ending on the date of the issuance of a lease for the Federal land.

(4) DILIGENT DEVELOPMENT REQUIREMENTS.—In issuing a lease under this subsection, the Secretary shall include work requirements and mandatory milestones—

(A) to ensure that diligent development is carried out under the lease; and

(B) to reduce speculative behavior.

(5) LAND MANAGEMENT.—The Secretary shall—

(A) establish the duration of leases issued under this subsection;

(B) include provisions in the lease requiring the holder of a lease granted under this subsection—

(i) to furnish a reclamation bond or other form of security determined to be appropriate by the Secretary;

(ii) on completion of the activities authorized by the lease—

(I) to restore the Federal land that is subject to the lease to the condition in which the Federal land existed before the lease was granted; or

(II) to conduct mitigation activities if restoration of the land to the condition described in subclause (I) is impracticable; and

(iii) to comply with such other requirements as the Secretary considers necessary to protect the interests of the public and the United States; and

(C)(i) establish best management practices to ensure the sound, efficient, and environmentally responsible development of solar resources on the Federal land in a manner that would avoid, minimize, and mitigate actual and anticipated impacts to habitat and ecosystem function resulting from the development; and

(ii) include provisions in the lease requiring renewable energy operators to comply with the practices established under clause (i).

(d) ROYALTIES.—

(1) IN GENERAL.—The Secretary shall establish royalties, fees, rentals, bonuses, and any other payments the Secretary determines to be appropriate to ensure a fair return to the United States for any lease issued under this section.

(2) RATE.—Any lease issued under this section shall require the payment of a royalty established by the Secretary by regulation in an amount that is equal to a percentage of the gross proceeds from the sale of electricity at a rate that—

(A) encourages production of solar energy;

(B) ensures a fair return to the public comparable to the return that would be obtained on State and private land; and

(C) encourages the maximum energy generation practicable using the least amount of land and other natural resources, including water.

(3) ROYALTY RELIEF.—To promote the maximum generation of renewable energy, the Secretary may provide that no royalty or a reduced royalty is required under a lease for a period not to exceed 5 years beginning on the date on which generation is initially commenced on the Federal land subject to the lease.

(4) DISPOSITION OF PROCEEDS.—

(A) IN GENERAL.—Of the amounts collected as royalties, fees, rentals, bonuses, or other payments under a lease issued under this section—

(i) 25 percent shall be paid by the Secretary of the Treasury to the State within the boundaries of which the income is derived;

(ii) 25 percent shall be paid by the Secretary of the Treasury to the 1 or more counties within the boundaries of which the income is derived;

(iii) 15 percent shall—

(I) for the period beginning on the date of enactment of this Act and ending on the date specified in subclause (II), be deposited in the Treasury of the United States to help facilitate the processing of renewable energy permits by the Bureau of Land Management in the State, subject to subparagraph (B)(i)(I); and

(II) beginning on the date that is 10 years after the date of enactment of this Act, be deposited in the Fund; and

(iv) 35 percent shall be deposited in the Fund.

(B) LIMITATIONS.—

(i) RENEWABLE ENERGY PERMITS.—For purposes of subclause (I) of subparagraph (A)(iii)—

(I) not more than $10,000,000 shall be deposited in the Treasury at any 1 time under that subclause; and

(II) the following shall be deposited in the Fund:

(aa) Any amounts collected under that subclause that are not obligated by the date specified in subparagraph (A)(iii)(II).

(bb) Any amounts that exceed the $10,000,000 deposit limit under subclause (I).

(ii) FUND.—Any amounts deposited in the Fund under clause (i)(II) or subparagraph (A)(iii)(II) shall be in addition to amounts deposited in the Fund under subparagraph (A)(iv).

(5) RENEWABLE ENERGY MITIGATION AND FISH AND WILDLIFE FUND.—

(A) ESTABLISHMENT.—There is established in the Treasury of the United States a fund, to be known as the ''Renewable Energy Mitigation and Fish and Wildlife Fund'', to be administered by the Secretary, for use in the State.

(B) USE OF FUNDS.—Amounts in the Fund shall be available to the Secretary, who may make the amounts available to the State or other interested parties for the purposes of—

(i) mitigating impacts of renewable energy on public land, with priority given to land affected by the solar development zones designated under this Act, including—

(I) protecting wildlife corridors and other sensitive land; and

(II) fish and wildlife habitat restoration; and

(ii) carrying out activities authorized under the Land and Water Conservation Fund Act of 1965 (16 U.S.C. 460l-4 et seq.) in the State.

(C) AVAILABILITY OF AMOUNTS.—Amounts in the Fund shall be available for expenditure, in accordance with this paragraph, without further appropriation, and without fiscal year limitation.

(D) INVESTMENT OF FUND.—

(i) IN GENERAL.—Any amounts deposited in the Fund shall earn interest in an amount determined by the Secretary of the Treasury on the basis of the current average market yield on outstanding marketable obligations of the United States of comparable maturities.

(ii) USE.—Any interest earned under clause (i) may be expended in accordance with this paragraph.

(e) PRIORITY DEVELOPMENT.—

(1) IN GENERAL.—Within the County, the Secretary shall give highest priority consideration to implementation of the solar lease sales provided for under this Act.

(2) EVALUATION.—The Secretary shall evaluate other solar development proposals in the County not provided for under this Act in consultation with the State, County, and other interested stakeholders.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 549—CONGRATULATING THE CHICAGO BLACKHAWKS ON WINNING THE 2010 STANLEY CUP

Mr. DURBIN (for himself and Mr. BURRIS) submitted the following resolution; which was referred to the Committee on the Judiciary:

S. RES. 549

Whereas, on June 9, 2010, the Chicago Blackhawks hockey team won the Stanley Cup;

Whereas the 2010 Stanley Cup win is the first Stanley Cup win for the Blackhawks since 1961, when John F. Kennedy was president and the Peace Corps was first established;

Whereas the Blackhawks joined the National Hockey League in 1926 and have a rich history in the League;

Whereas the Blackhawks were 1 of the original 6 teams in the National Hockey League;

Whereas, during a very difficult period for the National Hockey League, the Blackhawks remained a strong and competitive team, winning the Stanley Cup in 1934, 1938, and 1961;

Whereas the Stanley Cup championship appearance in 2010 is the first for the Blackhawks since 1992;