of Defense share of expenses under the National Guard Youth Challenge Program.

S. 658

At the request of Mr. TESTER, the names of the Senator from Arkansas (Mrs. LINCOLN) and the Senator from Illinois (Mr. BURRIS) were added as cosponsors of S. 658, a bill to amend title 38, United States Code, to improve health care for veterans who live in rural areas, and for other purposes.

S. 663

At the request of Mr. NELSON of Nebraska, the names of the Senator from New Jersey (Mr. LAUTENBERG) and the Senator from Connecticut (Mr. LIEBERMAN) were added as cosponsors of S. 663, a bill to amend title 38, United States Code, to direct the Secretary of Veterans Affairs to establish the Merchant Mariner Equity Compensation Fund to provide benefits to certain individuals who served in the United States merchant marine (including the Army Transport Service and the Naval Transport Service) during World War II.

S. 700

At the request of Mr. BINGAMAN, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 700, a bill to amend title II of the Social Security Act to phase out the 24-month waiting period for disabled individuals to become eligible for Medicare benefits, to eliminate the waiting period for individuals with life-threatening conditions, and for other purposes.

S. 714

At the request of Mr. WEBB, the name of the Senator from Iowa (Mr. HARKIN) was added as a cosponsor of S. 714, a bill to establish the National Criminal Justice Commission.

S. 731

At the request of Mr. NELSON of Nebraska, the names of the Senator from Illinois (Mr. BURRIS), the Senator from Missouri (Mrs. MCCASKILL), the Senator from Idaho (Mr. RISCH) and the Senator from Oregon (Mr. WYDEN) were added as cosponsors of S. 731, a bill to amend title 10, United States Code, to provide for continuity of TRICARE Standard coverage for certain members of the Retired Reserve.

S. 738

At the request of Ms. LANDRIEU, the name of the Senator from Georgia (Mr. CHAMBLISS) was added as a cosponsor of S. 738, a bill to amend the Consumer Credit Protection Act to assure meaningful disclosures of the terms of rental-purchase agreements, including disclosures of all costs to consumers under such agreements, to provide certain substantive rights to consumers under such agreements, and for other purposes.

S. 781

At the request of Mr. ROBERTS, the names of the Senator from Wyoming (Mr. ENZI) and the Senator from Tennessee (Mr. CORKER) were added as cosponsors of S. 781, a bill to amend the Internal Revenue Code of 1986 to provide for collegiate housing and infrastructure grants.

S. 795

At the request of Mrs. LINCOLN, the name of the Senator from Ohio (Mr. BROWN) was added as a cosponsor of S. 795, a bill to amend the Social Security Act to enhance the social security of the Nation by ensuring adequate public-private infrastructure and to resolve to prevent, detect, treat, intervene in, and prosecute elder abuse, neglect, and exploitation, and for other purposes.

S. 828

At the request of Mr. HARKIN, the name of the Senator from Iowa (Mr. GRASSLEY) was added as a cosponsor of S. 828, a bill to amend the Energy Policy Act of 2005 to provide loan guarantees for projects to construct renewable fuel pipelines, and for other purposes.

S. 831

At the request of Mr. KERRY, the name of the Senator from Iowa (Mr. HARKIN) was added as a cosponsor of S. 831, a bill to amend title 10, United States Code, to include service after September 11, 2001, as service qualifying for the determination of a reduced eligibility age for receipt of nonregular service retired pay.

S. 832

At the request of Mr. NELSON of Florida, the name of the Senator from Oklahoma (Mr. INHOFE) was added as a cosponsor of S. 832, a bill to amend title 36, United States Code, to grant a Federal charter to the Military Officers Association of America, and for other purposes.

S. 835

At the request of Mr. BROWNBACK, the name of the Senator from Iowa (Mr. GRASSLEY) was added as a cosponsor of S. 835, a bill to require automobile manufacturers to ensure that not less than 80 percent of the automobiles manufactured or sold in the United States by each such manufacturer to operate on fuel mixtures containing 85 percent ethanol, 85 percent methanol, or biodiesel.

S. 886

At the request of Mr. NELSON of Florida, the name of the Senator from Florida (Mr. MARTINEZ) was added as a cosponsor of S. 886, a bill to establish a program to provide guarantees for debt issued by State catastrophe insurance programs to assist in the financial recovery from natural catastrophes.

S. CON. RES. 14

At the request of Mrs. LINCOLN, the name of the Senator from North Carolina (Mr. BURR) was added as a cosponsor of S. Con. Res. 14, a concurrent resolution supporting the Local Radio Freedom Act.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. REID (for Mr. KENNEDY (for himself, Mr. LEAHY, Ms. SNOWE, Ms. COLLINS, Mr. SPECTER, Mr. SCHUMER, Mr. DURBIN, Mrs. FEINSTEIN, Mr. LEVIN, Ms. MIKULSKI, Mr. WHITEHOUSE, Mr. CARDIN, Ms. KLOBUCHAR, Mr. LIEBERMAN, Mrs. GILLIBRAND, Mr. MERKLEY, Mr. REED, Mr. NELSON, of Florida, Mr. KERRY, Mr. BINGAMAN, Mr. DODD, Mr. BAYH, Mr. UDALL of Colorado, Mrs. SHAHEEN, Mr. HARKIN, Mr. BROWN, Mrs. MURRAY, Mr. CASEY, Mr. JOHNSON, Mr. LAUTENBERG, Mr. NELSON of Nebraska, Ms. LANDRIEU, Ms. CANTWELL, and Mr. AKAKA)):

S. 909. A bill to provide Federal assistance to States, local jurisdictions, and Indian tribes to prosecute hate crimes, and for other purposes; to the Committee on the Judiciary.

Mr. KENNEDY. Mr. President, hate crimes harm innocent victims, terrorize entire communities, and threaten the very fabric of our nation. They send a poisonous message that some Americans deserve to be victimized solely because of who they are or who they are perceived to be. Hate crimes offend the fundamental ideals on which Nation was founded. They can not be tolerated in any free society, and it is long past time to enact legislation to correct the deficiencies in the current federal hate crimes statute.

For far too long, law enforcement has been forced to investigate hate crimes with one hand tied behind its back. Now is the time to change this. This bill strengthens the Federal Government's ability to investigate and prosecute hate crimes. It removes the excessive restrictions currently existing in federal law. It offers Federal assistance for investigating and prosecuting hate crimes to State and local law enforcement. It provides training grants for local law enforcement to combat hate crimes committed by juveniles.

The first Federal hate crimes statute was passed over 40 years ago in 1968, soon after the assassination of Dr. Martin Luther King, Jr. It authorized the Federal Government to investigate and prosecute crimes committed against individuals because of their race, color, religion, or national origin. The original statute was a major advance in the march of progress, but it is now a generation out of date.

The time has come to stand up for all victims of hate crimes—victims like Matthew Shepard, for whom this bill is named. Matthew died a horrible death in 1998 at the hands of two men who singled him out because of his sexual orientation. Since Matthew's murder, his mother has worked courageously to make sure that we never forget the suffering that her son endured, and to remind Congress that it has a responsibility to protect individuals like her son. Yet today, more than 10 years after Matthew's death—10 years—we still have not modernized our hate crimes laws. How long are we going to wait?

The bill we are introducing today expands the current hate crimes statute

and gives Federal, State, local, and tribal authorities greater ability to investigate and prosecute hate crimes effectively. The bill closes flagrant loopholes in the current statute that prevent or undermine the prosecution of the individuals who commit these vicious crimes.

This bill broadens the original Federal hate crimes statute by prohibiting crimes based on a victim's actual or perceived sexual orientation, gender, gender identity, or disability.

According to FBI statistics, hate crimes based on sexual orientation make up approximately 17 percent of all hate crimes. Considering that gays and lesbians make up approximately 3 percent of the population, the FBI statistics suggest that gays and lesbians are victimized at a rate approximately 6 times higher than that of the average American. Research suggests that hate-motivated violence against gay, lesbian, bisexual, and transgender citizens is particularly extreme. As these statistics and the research make clear, hate crimes are a very real danger to gay, lesbian, bisexual, and transgender citizens. We must act—without further delay—to correct these unacceptable deficiencies in current law and protect all citizens from these brutal crimes.

Our bill also increases the Federal Government's ability to prosecute hate crimes. It removes the prerequisite that a victim be engaged in a ''federally protected activity'' before the Federal Government can prosecute an offender under the statute. This restrictive provision is outdated, unwise, and unnecessary, particularly when one considers the unjust outcomes that can result from limiting prosecution to offenders to target victims participating in one or more of the following 6 narrow categories of federally protected activity: attending or enrolling in a public school or public college; participating in a benefit, service, privilege, program, facility or activity administered by a state or local government; applying for or working in private or state employment; serving as a juror in a state court; using a facility of interstate commerce or a common carrier; or enjoying public accommodations or places of exhibition or entertainment. We know that individuals may be victimized while engaging in activities that are not included in this list of activities—they could be victims while engaging in routine activities, going about their normal day. Americans should be protected from hate crimes in everything they do. There should be no distinction between hate crimes occurring while a victim is engaged in a routine activity or one of the six specified federally protected activities described above.

This bill corrects a gap in the current hate crimes statute that limits prosecution to offenders who interfere with a victim's participation in certain federally protected activities. In June 2003, six Latino teenagers went to a family restaurant on Long Island. The teenagers knew one another from involvement in community activities and have come together to celebrate a birthday. As the group entered the restaurant, three men who were leaving the bar assaulted the teenagers, pummeling one boy and severing a tendon in his hand with a sharp weapon. During the attack, the men yelled racial slurs and one identified himself as a skinhead. Two of the men were tried under the current Federal hate crimes law and were acquitted. The jurors said they acquitted the offenders because the Government failed to prove that using a restaurant was a federally protected activity. The result in this case is just one example of the inadequate protections provided under current law. The bill we introduce today will eliminate the federally protected activity requirement and give jurors greater ability to convict all perpetrators of hate crimes.

The bill modernizes the Federal Government's ability to prosecute hate crimes, but it fully respects the primary role of state, local, and tribal law enforcement authorities in responding to hate crimes in their jurisdictions. The bill protects these local interests with a strict certification process, which requires the Federal Government to consult with state and local officials before prosecuting a Federal case. In accord with certification, it is our belief that the vast majority of hate crimes will continue to be prosecuted at the State and local level.

In addition, our bill authorizes the Justice Department to increase the number of Department personnel to prevent and respond to hate crimes. This increase will enable Federal authorities to develop the manpower necessary to act effectively to prevent and respond to hate crimes.

The bill also authorizes the Justice Department to provide needed investigative resources to state and local law enforcement during these challenging economic times. This expansion of federal assistance is meant to supplement, not supplant, the efforts of state and local law enforcement authorities, so that hate crimes can be effectively investigated and prosecuted in the future.

Hate crimes investigations tend to be expensive, requiring considerable law enforcement effort, and extensive use of grand juries. The bill expands the Justice Department's opportunity to provide support for these expenses. It authorizes the Attorney General to offer grants of up to $100,000 to help state, local, and tribal law enforcement officials manage the high costs of investigating and prosecuting hate crimes. It also authorizes the Justice Department to award grants to State, local, and tribal authorities for programs that combat hate crimes committed by juveniles, including programs designed to train local law enforcement officers in identifying, investigating, prosecuting and preventing hate crimes. These measures will help ensure that state and local authorities have the resources necessary to successfully combat and prosecute hate crimes.

Collecting data on hate crimes is important for analyzing crime trends and tailoring effective criminal policy. Our bill increases the Federal Government's ability to monitor hate crimes by requiring the FBI to increase the statistics it collects about such crimes. Currently, the FBI collects hate crimes data on race, religion, sexual orientation, ethnic background, and disability. Our bill requires the FBI to collect new statistics on hate crimes based on an individual's gender or gender-identity, and hate crimes committed by juveniles. By increasing the amount of data collected by the FBI, we will be able to better understand the gravity of the hate crimes committed in our communities.

Hate crimes are a festering problem, causing terror in neighborhoods across America. According to the most recent statistics released by the FBI, there were at least 9,527 victims of hate-motivated crimes in 2007. Based on that number, an average of 26 victims per day were terrorized as a consequence of their race, religion, sexual orientation, ethnic background, or disability. The FBI's statistics reveal that race-related hate crimes are the most common type of hate crimes, comprising approximately 50 percent of all hate crimes reported to the FBI. That said, crimes based on religion, sexual orientation, and ethnic background occur with alarming frequency as well.

These hate crimes statistics are disturbing, but they represent only the tip of the iceberg of hate crimes occurring in America. The Southern Poverty Law Center, the Human Rights Campaign, and the US Bureau of Justice Statistics agree that the FBI's hate crimes numbers do not reflect the actual number of hate crimes occurring in our communities each year. The Southern Poverty Law Center estimates that the annual number of hate crimes committed in the U.S. is close to 50,000. In addition, the Human Rights Campaign states that a hate crime occurs every 6 hours. Survey data from the Bureau of Justice Statistics' biannual National Crime Victimization Survey estimates that an average of 191,000 hate crime victimizations take place each year. Based on this survey, over 540 people are victimized each day, based on their race, religion, sexual orientation, ethnic background, or disability—more than 22 victims per hour. These statistics are not just shocking—they are shameful. It is time for Congress to specifically address the serious problem of hate crimes in America.

In addition to the legal impact of this bill, its symbolic impact is equally important. This bill emphasizes the devastatingly unique nature of hate crimes. It says we recognize that hate crimes provide aggressors with the means to attack an entire community

through a single act of violence, and send a message of fear that vastly transcends the immediate crime and its victim. It shows we understand that hate crime offenders should be prosecuted for committing a crime against an entire community. After so many years of inaction, we in Congress have an obligation to demonstrate that we understand how hate crimes affect our nation's communities.

It takes only a brief survey of any major news outlet to find horrifying stories of hate crimes and the inability of law enforcement to prosecute offenders for their acts of hate. The 1999 murder of four women in Yosemite National Park graphically illustrates the need to include gender in our hate crimes statute. These four women were murdered by a man who admitted having fantasized about killing women for most of his life. These women lost their lives for one reason—because they were women. We need to send a clear message that we will not accept such acts of hate. Without this bill, however, such a crime cannot be federally prosecuted as a hate crime.

Gender identity must also be included in our definition of those characteristics protected by a hate crimes statute. Many are familiar with the story of Brandon Teena, who was raped and beaten in Humboldt, Nebraska in 1993 by two male friends after they discovered that he was living as a male but was anatomically female. The local sheriff refused to arrest the offenders, and they later shot and stabbed Brandon to death.

A more recent, less well-known incident occurred when Fred C. Martinez Jr., a Navajo transgender youth, was murdered while walking home from a party. Fred was killed for one reason alone—because he was a transgender youth. By passing this bill, the Senate will send a strong message that hate crimes based on sexual identity are unacceptable and perpetrators of such crimes will face tough criminal penalties under Federal law.

Hate crimes against disabled Americans are very disturbing and deserve protection at the Federal level as well. In October 2002, two deaf girls, one of whom was wheelchair bound due to cerebral palsy, were harassed and sexually assaulted by four suspected gang members in a local park. The girls were attacked because they were disabled and unable to defend themselves. Although the alleged perpetrators were prosecuted, the assaults could not be charged as hate crimes because no State or Federal protections for disability-based hate crimes existed in Federal or State law. This must change.

These are only a few examples of the hate perpetrated against individuals in America based on their sexual orientation, gender, gender identity, and disability. We can no longer allow any of these communities to live in fear. Crimes based on an individual's sexual orientation, gender, gender identity, or disability must be prosecuted for what they are—crimes of hate.

Individuals should not only be protected from hate crimes because of their actual characteristics; they must also be protected from hate crimes based on the inaccurate perceptions of others. Last year in Brooklyn, New York, Jose Sucuzhanay was walking arm in arm with his brother, Romel Sucuzhanay, after attending a church party. According to officials, about half a block from Jose's home, a black sports utility vehicle drove by and the two men in the vehicle began shouting what witnesses described as vulgarisms against Hispanics and gay men. The car stopped and one of the two men approached Jose and smashed a beer bottle over the back of his head. The other man then took an aluminum baseball bat from the rear of the vehicle and repeatedly struck Jose on his shoulder, ribs, and back. Once Jose fell to the ground, he received several full-forced, crushing blows to his head with the aluminum baseball bat. Jose, a father of two and local real estate agent, died 5 days later because of the hate-motivated attack. He did not deserve to lose his life because he was perceived to be gay. That is why the bill we are introducing today criminalizes crimes based on the perceived characteristics of a victim.

We also know that hate crimes covered by current Federal law—based on race, religion, national origin, and color—still occur and must be prosecuted. Following the 2008 presidential election, three men in New York went on a rampage attacking African-American residents of Staten Island in response to the historic election of President Barack Obama. The men attacked one 17-year-old African-American man with a metal pipe and collapsible baton. They attacked another African-American man by pushing him to the ground. They assaulted still another man, whom they mistakenly believed was African-American, by mowing him down with a car while yelling racial epithets at him. Clearly, this demonstrates that race-based violence is continuing at an unacceptable level, and we must act to help law enforcement more vigorously deal with hate crimes.

Hate crimes legislation has the support of President Obama, a majority of Congress, 26 State Attorneys General, and a broad coalition of law enforcement, civic, religious, and civil rights groups. Recent history shows that Congress is ready to make hate crimes legislation into law. In 2007, the Senate voted 60 to 39 in support of a similar hate crimes bill. An equally powerful statement was made by the House when it voted 237 to 180 for the hate crimes bill introduced that year. As a Senator, President Obama voted to support hate crimes legislation. Now, as President, he has included the expansion of hate crimes in his civil rights agenda. The political will of our Nation is clear—it is time for this bill to become law.

Over 300 law enforcement, civil rights, civic, and religious organizations have endorsed our bill, including the International Association of Chiefs of Police, the National District Attorneys Association, the National Sheriffs Association, the Police Executive Research Forum, the Leadership Conference on Civil Rights, the Anti-Defamation League, the Human Rights Campaign, and the Interfaith Alliance. All these diverse groups have come together to say that now is the time for us to protect our fellow citizens from the brutality of hate-motivated violence. They strongly support this legislation because they know it is a balanced and sensible approach that will bring greater protection to our citizens, along with much-needed resources for local and State law enforcement fighting hate crimes.

Passing this bill will send a message, loud and clear, that those who victimize individuals because of their race, color, religion, national origin, sexual orientation, gender, gender identity, or disability will go to prison. In addition, passing this bill will provide Federal, State, local, and tribal authorities with stronger means to prosecute crimes of hate. It has been over 10 years since Matthew Shepard was left to die on a fence in Wyoming because of who he was. It has also been 10 years since this bill was initially considered by Congress. In those 10 years, we have gained the political and public support that is needed to make this bill become law. Today, we have a President who is prepared to sign hate crimes legislation into law, and a Justice Department that is willing to enforce it. We must not delay the passage of this bill. Now is the time to stand up against hate-motivated violence and recognize the shameful damage it is doing to our Nation.

Mr. LEAHY. Mr. President, this is National Crime Victims' Rights Week—a time when communities in Vermont and across the Nation recognize the needs of crime victims, and work together to promote victims' rights and services. There is no more important time than now to renew our commitment to address the needs of crime victims and their families.

Today, I am pleased to join Senator KENNEDY, Senator COLLINS, and more than 30 other Senators from both sides of the aisle to reintroduce the Matthew Shepard Hate Crimes Prevention Act of 2009. This is a bipartisan bill designed to combat crimes that have long terrorized communities and remain a serious problem in this country. This legislation is a matter of simple justice. It is past time for Congress to enact this bill and strengthen the Federal Government's role in preventing and punishing crimes motivated by hate.

I commend Senator KENNEDY for his leadership over the last decade in working to expand our Federal hate crimes law, and I am proud to once again be an original cosponsor of this legislation. A bipartisan majority of

the Members in the House of Representatives voted to pass this legislation in the last Congress. Unfortunately, there were partisan attempts to filibuster and prevent passage of the Senate bill. The measure was ultimately attached to the Department of Defense Authorization bill with the bipartisan support of 60 Senators. While I am disappointed that the hate crime provision was taken out of that bill at conference, I am hopeful that our efforts to enact this civil rights measure into law will be successful this year.

Violent crimes motivated by prejudice and hate are tragedies that haunt American history. From the lynchings that plagued race relations for more than a century, to the well-publicized slayings of Matthew Shepard and James Byrd, Jr., in the 1990s, this is a story that we have heard too often in this country. Unfortunately, in my home state of Vermont, there have been two attacks in recent years that appear to have been motivated by the victims' religion or sexual orientation.

Perhaps the most persuasive evidence that hate crimes are becoming more prevalent and more nationalized is a leaked copy of the Department of Homeland Security report on violent extremism in the United States. The report is nothing short of chilling.

The DHS report found that ''the economic downturn and the election of the first African American president present unique drivers for rightwing radicalization and recruitment'' and these elements in turn have the potential to drive hate groups to carry out violence. It also found that anti-immigrant fervor by organized hate groups ''has the potential to turn violent.'' The DHS report concluded that the ''advent of the Internet'' has potentially made ''extremist individuals and groups more dangerous and the consequences of their violence more severe.''

Of course, these findings comport with a recent Southern Poverty Law Center, SPLC, report on hate group activity in the United States entitled ''The Year in Hate.'' The SPLC repot found that activity by known domestic hate groups has increased by 50 percent since 2000, from 602 hate groups in 2000, to 926 hate groups in 2008. The recent and rapid growth in hate group activity is simply astonishing.

It remains painfully clear that as a Nation, we still have serious work to do in protecting all Americans from these crimes and in ensuring equal rights for all our citizens. While the answer to hate and bigotry must ultimately be found in increased tolerance, strengthening our Federal hate crimes laws is a step in the right direction.

The Matthew Shepard Hate Crimes Prevention Act of 2009 improves existing law by making it easier for Federal authorities to investigate and prosecute crimes based on race, color, religion, and national origin. Victims will no longer have to engage in a narrow range of activities, such as serving as a juror, to be protected under Federal law. This bill also expands Federal protections to include the problem of hate crimes committed against people because of their sexual orientation, gender, gender identity, or disability, which is a key and long-overdue expansion of protection. Finally, this bill provides assistance and resources to state, local, and tribal law enforcement to address hate crimes.

This bill strengthens Federal jurisdiction over hate crimes as a back-up, but not a substitute, for state and local law enforcement. States will still bear primary responsibility for prosecuting most hate crimes, which is important to me as a former state prosecutor. In a sign that this legislation respects the proper balance between Federal and local authority, it has received strong bipartisan support from state and local law enforcement organizations across the country.

Moreover, this bill accomplishes the critically important goal of protecting all of our citizens without compromising our constitutional responsibilities. It is a tool for combating acts and threats of violence motivated by hatred and bigotry. But it does not target pure speech, however offensive or disagreeable. The Constitution does not permit us in Congress to prohibit the expression of an idea simply because we disagree with it. To paraphrase Justice Oliver Wendell Holmes, the Constitution protects not only freedom for the thought and expression we agree with, but freedom for the thought that we hate. I am devoted to that principle, and I am confident that this bill does not contradict it.

We crafted this legislation after long and thoughtful consultation with many of the advocates who work so hard to promote civil rights and with Justice Department attorneys in the field who work on hate crimes prosecutions every day. It contains changes to Federal hate crime law that will improve the law's operation and implementation. I want to thank the Leadership Conference on Civil Rights, Human Rights First, and the more than 300 law enforcement, civil rights, religious, and other professional organizations for their assistance with and support for this legislation, and for their tireless work on behalf of hate crimes victims in the United States.

The crimes targeted in this bill are particularly pernicious crimes that affect more than just their victims and those victims' families. They inspire fear in those who have no connection to the victim other than a shared characteristic such as race or sexual orientation. That is wrong. All Americans have the right to live, travel and gather where they choose. In the past we have responded as a Nation to deter and to punish violent denials of civil rights. We have enacted Federal laws to protect the civil rights of all of our citizens for nearly 150 years.

The Matthew Shepard Hate Crimes Prevention Act continues that great and honorable tradition, and brings us one step closer towards ensuring an America that values tolerance and protects all of its people. I hope all Senators will support passing this important bipartisan bill this year.

Mrs. FEINSTEIN. I wish today to support the Matthew Shepard Hate Crimes Prevention Act of 2009. I want to thank and commend my friend and colleague, Senator KENNEDY, for his leadership and dedication on this important issue. It is long past time that we move to bring existing Federal hate crimes law into the 21st century.

I have been an original cosponsor of the Hate Crimes Prevention Act since it was first introduced in the Senate over a decade ago.

And I am proud to join today with my colleagues—Senators KENNEDY, LEAHY, SPECTER, COLLINS, SNOWE, SCHUMER, DURBIN, and others—to reintroduce this legislation, which will once and for all send a message: We will no longer turn a blind eye to hate crimes in this country.

This legislation is a crucial step toward prosecuting crimes directed at thousands of individuals who are the targets of brutal and senseless violence.

The current Federal hate crimes law simply does not go far enough. It covers only crimes motivated by bias on the basis of race, color, religion or national origin.

This bill improves the current Federal hate crime law by including crimes motivated by gender, gender identity, sexual orientation, and disability.

Specifically, the Matthew Shepard Crimes Prevention Act of 2009 expands on the 1968 definition of a hate crime.

Under current Federal law, hate crimes only cover attacks based on race, color, religion, and national origin.

Under the proposed bill, hate crimes will include: gender, gender identity, sexual orientation, and disability.

The bill enables States, local jurisdictions, and Indian tribes to apply for Federal grants in order to solve hate crimes and provides Federal agents with broader authority to aid State and local police.

Additionally, the bill amends the Hate Crime Statistics Act to allow law enforcement agencies to gather additional data on violent crimes committed out of hate.

The bill also includes a ''Rule of Construction'' to ensure that it does not intrude on first amendment protected rights to freedom of speech.

I believe that it is time for Congress to expand the ability of the Federal Government to investigate and prosecute anyone who would target victims because of hate. In States that have already enacted hate crimes laws, the Federal Government must provide the resources to ensure that those crimes do not go unpunished. We can and must do more.

Across the Nation, horrific instances of violence are occurring that this bill

would work to fight against. I would like to share just a few examples:

In February 2008 in Oxnard, CA, Lawrence ''Larry'' King, a 15-year-old boy was shot and killed by a fellow classmate at his junior high school. Larry, who had told his classmates he was gay, had long been harassed and bullied at school. The way he was treated is unacceptable, and his death was a tragic and poignant reminder of why it is so important to stop bullying and violence in our schools.

In Laurel, DE, earlier this month, three teenagers were charged with robbing and assaulting a 31-year-old developmentally disabled man. The victim was walking home one Friday evening from his brother's house in the Laurel Village Mobile Home Park and was dragged into a wooden area, beaten, and robbed of his wallet and keys. The victim's mother later found him and took him to the hospital where he was treated for a concussion.

Lastly, one of the most well-known cases in California happened in West Hollywood to actor Trev Broudy in 2002. The night of the attack, Trev Broudy was hugging a man on a street. Three men with a baseball bat savagely attacked the actor and left him in a coma for approximately 10 weeks. As a result of the attack, Trev suffered brain damage, lost half of his vision, and has experienced trouble hearing.

The crimes are brutal. The attackers targeted their victims because of who they are. Yet, none of these crimes can be prosecuted as a Federal hate crime.

These are not isolated instances.

These crimes occur all too often.

According to the latest FBI statistics, there were almost 7,700 hate crime incidents in the United States in 2007. Of those, 1,789 occurred in California, with 15 percent of those based on sexual orientation.

Nationally, approximately 50.8 percent were motivated by racial bias, 18 percent were motivated by religious bias, 17 percent were motivated by sexual orientation, and 13.2 percent were motivated by ethnicity or national origin bias. One percent involved a bias against a disability.

Even more disturbing is the fact that these FBI statistics show only a fraction of the problem because so many hate crimes are unreported.

The Southern Poverty Law Center, a nonprofit organization located in Montgomery, AL and internationally known for its tolerance education programs, estimates that the actual number of hate crimes committed in the United States each year is closer to 50,000 as opposed to the nearly 8,000 cases reported to the FBI.

A close analysis of hate crimes rates demonstrates that groups that are now covered by current laws—such as African Americans, Muslims, and Jews, report similar rates of hate crimes victimizations as gays and lesbians—who are not currently protected.

Every person's life is valuable. Congress must act to protect every individual who is targeted simply because of who they are.

We must also stop the way that hate crimes terrorize communities. When people are targeted because of who they are, they often live in fear and communities suffer from tension and a lack of trust. These are crimes that damage our social fabric, and we must send a clear message that we cannot tolerate this kind of intimidation in the United States.

This is not a new bill. It was first introduced in 1998. It has passed the Senate numerous times: in 2000, 2002, and 2004 as an amendment to the Department of Defense, Authorization bill. It has also passed the House in 2007 as a stand-alone bill and in 2006 as an amendment to the Adam Walsh Act. But still, it has not been enacted into law.

In addition, last Congress, this body passed this legislation favorably as an amendment to the Defense authorization bill, but the amendment was removed from the final version of the bill that the President signed.

This legislation is bipartisan and has broad coalition support. It is supported by 26 State attorneys general and over 300 law enforcement, professional, educational, civil rights, religious, and civic organizations.

I hope that my colleagues will join me in supporting it and working to enact it into law in this Congress.

Let us send a message to all Americans that we will not turn a blind eye to hate crimes and will instead support the values of tolerance and community that unite us as Americans.

By Mr. MERKLEY:

S. 911. A bill to amend the Truth in Lending Act to prohibit prepayment penalties, and for other purposes; to the Committee on Banking, Housing, and Urban Affairs.

Mr. MERKLEY. Mr. President, I am introducing two pieces of legislation to address the very heart of our economic crisis—the housing market and the deceptive lending practices that have placed millions of homes at risk of foreclosure.

In the last few years, millions of families were led into unsustainable home mortgages that pushed our country into an economic crisis unprecedented in our lifetimes. Instead of fulfilling a dream and contributing to a secure financial future, home mortgages have too often become a check for stripping wealth from working Americans.

These two bills, the Transparency for Homeowners Act, S. 911, and the Promoting Mortgage Responsibility Act, S. 912, will put an end to deceptive and unfair mortgage practices that played a pivotal role in tricking American families to accept risky and unsustainable mortgages.

Two key factors drew families into these mortgages that paved the way for this recession. First, steering payments.

Steering payments were paid to brokers who enticed unsuspecting homeowners into deceptive and expensive mortgages. These secret bonus payments, often called yield spread premiums, turned home mortgages into a scam. A family would go to a mortgage broker to get advice in getting the best possible loan. The family would trust the broker to give advice because, quite frankly, they were paying the broker for that service. But what the borrower did not realize is that the broker would earn thousands of bonus dollars from the lender if the broker could convince the homeowner to take out a high-priced mortgage, such as one with an exploding interest rate, rather than a plain vanilla 30-year fixed rate mortgage.

The second factor is prepayment penalties. Prepayment penalties added insult to injury. After the homeowners realized they had been steered into an unsustainable mortgage, they soon discovered that a large prepayment penalty made it too costly for them to refinance to a more affordable loan. They were locked into that first destructive loan they did not fully understand when it was presented.

This scam has had a tremendous impact. A study for the Wall Street Journal found that 61 percent of the subprime loans that originated in 2006—that is 61 percent that originated in 2006—went to families who qualified for prime loans. More than half the borrowers who qualified for a prime loan ended up with a subprime loan because of these steering payments, putting millions of American families at risk. This is simply wrong—a publicly regulated process designed to create a relationship of trust between families and brokers but that leaves borrowers unaware of payments that take place, putting them into expensive and destructive mortgages.

I call your attention to a New York Times editorial published on April 9 entitled ''Predatory Brokers.'' This editorial highlighted the problem. The Times concluded that:

> The first step must be to outlaw the kickbacks that lenders pay brokers for steering clients into costlier loans.

The editorial went on to say that:

> The most clearly unethical form of payment is the so-called yield-spread premium.

My friends, it is difficult to overstate the damage that has been done by these practices. An estimated 20,000 Oregon families will lose their homes to foreclosure in 2009. Nationwide, an estimated 2 million families will lose their homes this year. And the total of foreclosed families is predicted to reach 9 million by 2012.

The legislative solutions I propose are very simple. The bills I am introducing today will ensure these practices do not again haunt the mortgage business in America. First, the Transparency For Homeowners Act ends the secret steering payments to lenders who lead homeowners into deceptive mortgages they cannot afford over the long term. Second, the Promoting Mortgage Responsibility Act prohibits

lenders from issuing costly financial penalties that prevent homeowners from refinancing into a more affordable loan.

It is simple: an end to steering payments and an end to prepayment penalties. We should recognize that not only have these practices damaged the financial foundations for our families and millions of families at the retail level—turning the American dream of home ownership into an American nightmare—but these practices, which resulted in a huge surge in subprime lending, set the stage for the disaster that would come and is still unfolding on Wall Street and crippling economies around the world.

My legislation will restore transparency to the mortgage lending process and help make home ownership a stable investment for families once again. The time has come for us to make sure that secret steering payments and paralyzing prepayment penalties never again haunt American families. Let us restore the American dream of home ownership.

By Mr. CORNYN (for himself and Mr. HARKIN):

S. 913. A bill to amend the Internal Revenue Code of 1986 to expand workplace health incentives by equalizing the tax consequences of employee athletic facility use; to the Committee on Finance.

Mr. CORNYN. Mr. President, I rise to introduce the Workforce Health Improvement Program Act of 2009, otherwise known as the WHIP Act. This bipartisan bill I introduce today is the same legislation I introduced in the 110th Congress. I am very pleased to be joined again by my good friend and colleague, Senator TOM HARKIN, who shares my commitment to helping keep America fit.

Public health experts unanimously agree that people who maintain active and healthy lifestyles dramatically reduce their risk of contracting chronic diseases. And as the government works to reign in the high cost of health care, it is worth talking about what we all can do to help ourselves. As you know, prevention is key, and exercise is a primary component in the prevention of many adverse health conditions that can arise over one's lifetime. A physically fit population helps to decrease health-care costs, reduce governmental spending, reduce illnesses, and improve worker productivity.

According to the Centers for Disease Control and Prevention, CDC, the economic cost alone to businesses in the form of health insurance and absenteeism is more than $15 billion. Additionally, the CDC estimates that more than ⅓ of all US adults fail to meet minimum recommendations for aerobic physical activity based on the 2008 Physical Activity Guidelines for Americans. With physical inactivity being a key contributing factor to overweight and obesity, and adversely affecting workforce productivity, we quite simply need to do more to help employers encourage exercise.

Given the tremendous benefits exercise provides, I believe Congress has a duty to create as many incentives as possible to get Americans off the couch, up, and moving.

With this in mind, I am introducing the WHIP Act.

Current law already permits businesses to deduct the cost of on-site workout facilities, which are provided for the benefit of employees on a pretax basis. But if a business wants or needs to outsource these health benefits, they and/or their employees are required to bear the full cost. In other words, employees who receive off-site fitness center subsidies are required to pay income tax on the benefits, and their employers bear the associated administrative costs of complying with the IRS rules.

The WHIP Act would correct this inequity in the tax code to the benefit of many smaller businesses and their employees. Specifically, it would provide an employer's right to deduct up to $900 of the cost of providing health club benefits off-site for their employees. In addition, the employer's contribution to the cost of the health club fees would not be taxable income for employees—creating an incentive for more employers to contribute to the health and welfare of their employees.

The WHIP Act is an important step in reversing the largely preventable health crisis that our country is facing, through the promotion of physical activity and disease prevention. It is a critical component of America's health care policy: prevention. It will improve our Nation's quality of life by promoting physical activity and preventing disease. Additionally, it will help relieve pressure on a strained health care system and correct an inequity in the current tax code.

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. 913

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 ''Workforce Health Improvement Program Act of 2009''.

SEC. 2. EMPLOYER-PROVIDED OFF-PREMISES HEALTH CLUB SERVICES.

(a) TREATMENT AS FRINGE BENEFIT.—Subparagraph (A) of section 132(j)(4) of the Internal Revenue Code of 1986 (relating to on-premises gyms and other athletic facilities) is amended to read as follows:

''(A) IN GENERAL.—Gross income shall not include—

''(i) the value of any on-premises athletic facility provided by an employer to its employees, and

''(ii) so much of the fees, dues, or membership expenses paid by an employer to an athletic or fitness facility described in subparagraph (C) on behalf of its employees as does not exceed $900 per employee per year.''.

(b) ATHLETIC FACILITIES DESCRIBED.—Paragraph (4) of section 132(j) of the Internal Revenue Code of 1986 (relating to special rules) is amended by adding at the end the following new subparagraph:

''(C) CERTAIN ATHLETIC OR FITNESS FACILITIES DESCRIBED.—For purposes of subparagraph (A)(ii), an athletic or fitness facility described in this subparagraph is a facility—

''(i) which provides instruction in a program of physical exercise, offers facilities for the preservation, maintenance, encouragement, or development of physical fitness, or is the site of such a program of a State or local government,

''(ii) which is not a private club owned and operated by its members,

''(iii) which does not offer golf, hunting, sailing, or riding facilities,

''(iv) whose health or fitness facility is not incidental to its overall function and purpose, and

''(v) which is fully compliant with the State of jurisdiction and Federal anti-discrimination laws.''.

(c) EXCLUSION APPLIES TO HIGHLY COMPENSATED EMPLOYEES ONLY IF NO DISCRIMINATION.—Section 132(j)(1) of the Internal Revenue Code of 1986 is amended—

(1) by striking ''Paragraphs (1) and (2) of subsection (a)'' and inserting ''Subsections (a)(1), (a)(2), and (j)(4)'', and

(2) by striking the heading thereof through ''(2) APPLY'' and inserting ''CERTAIN EXCLUSIONS APPLY''.

(d) EMPLOYER DEDUCTION FOR DUES TO CERTAIN ATHLETIC FACILITIES.—

(1) IN GENERAL.—Paragraph (3) of section 274(a) of the Internal Revenue Code of 1986 (relating to denial of deduction for club dues) is amended by adding at the end the following new sentence: ''The preceding sentence shall not apply to so much of the fees, dues, or membership expenses paid to athletic or fitness facilities (within the meaning of section 132(j)(4)(C)) as does not exceed $900 per employee per year.''.

(2) CONFORMING AMENDMENT.—The last sentence of section 274(e)(4) of such Code is amended by inserting ''the first sentence of'' before ''subsection (a)(3)''.

(e) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after the date of the enactment of this Act.

By Mr. SPECTER:

S. 914. A bill to establish an independent Cures Acceleration Network agency, to sponsor promising translational research to bridge the gap between laboratory discoveries and life-saving therapies, to reauthorize the National Institutes of Health, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

Mr. SPECTER. Mr. President, the bill that I am introducing today would authorize the establishment of the Cures Acceleration Network, CAN. This new $2 billion agency would provide funds to translate research discoveries from the bench to the bedside and would operate as an independent agency. It would not be part of the Department of Health and Human Services. The CAN would make awards outside of the traditional funding stream to accelerate the development of cures and treatments including but not limited to drugs, devices, and behavioral therapies. The CAN would have a flexible expedited review process to get monies into the hands of the grantees as quickly as possible. These development

funds would complement the research dollars provided to the National Institutes of Health, NIH, and would not compete or take monies away from the NIH.

The bill also would raise the authorization level of the National Institutes of Health to $40 billion in fiscal year 2010, elevate the Center for Minority Health and Health Disparities to Institute status, and implement a new conflict-of-interest provision.

While the NIH funds much of the basic biomedical research at universities across the country, the CAN would take those findings found through basic research and provide funding to fill the gap between laboratory discoveries and life-saving medical therapies. This funding gap—often referred to as ''the valley of death'' arises after Federal basic-science support ends and before investors are willing to commit to a promising discovery. Very often finding funds to fill this gap is a daunting challenge, especially during a period of economic downturn, when investors have fewer resources to invest. This has had a severe impact on America's biotechnology industry.

The need for the CAN is clear: Capital raised by America's biotechnology companies fell 55 percent in 2008 compared to 2007. Also relative to 2007, 90 percent of small public biotechnology companies are now operating with less than 6 months of cash on hand. In the last 5 months alone, at least 24 U.S. public biotech companies have either placed drug development programs on hold or cut programs altogether. These companies have postponed clinical trials to treat melanoma, cervical cancer, lupus, chemotherapy side effects for breast cancer patients, multiple sclerosis, diabetes and atherosclerosis, drug trials to treat non-Hodgkin's lymphoma, testing of pandemic flu vaccine, trials to treat plaque psoriasis and heart disease, and a treatment for mesothelioma.

In short, without adequate funding—these companies will be unable to take these products to the development stage, the basic research done by the NIH will be lost, and many patients will die waiting for drugs and devices to give them a better quality of life.

The CAN would fund two types of grant awards, each with an authorization of $1 billion in the first year and additional funds in succeeding fiscal years.

The Cures Acceleration Grant Awards will provide grant awards of up to $15 million per year per project with out-year funding available. These awards would be available to applicants who do not have access to private matching funds.

The Cures Acceleration Partnership Awards also would provide grants for up to $15 million per year per project with additional funds available in the out-years. However, grant awards would require a match of three Federal dollars to one grantee dollar, as a way to partially offset development costs.

For both grant types, the CAN Board may waive the award limitation as well as modify the matching requirement.

Eligible grantees would include public or private entities such as institutions of higher education, medical centers, biotechnology companies, universities, patient advocacy organizations, pharmaceutical companies and academic research institutions.

To provide for expedited FDA approval, the grantees must also establish protocols that comply with FDA standards to meet regulatory requirements at all stages of development, manufacturing, review, approval and safety surveillance of a medical product.

The provisions of the Bayh-Dole Act would apply.

The CAN grant proposals would be evaluated by a 24-member board comprised of experienced individuals of distinguished achievement, and representative of a broad range of disciplinary interests including: venture capitalists and business executives with experience in managing scientific enterprises; scientists with expertise in the fields of basic research, biopharmaceuticals, drug discovery, drug delivery of medical products, bioinformatics, gene therapy or medical instrumentation, regulatory review and approval of medical products; and representatives of patient advocacy organizations.

The Chairman and Vice Chairman of the CAN shall be appointed by the President with the advice and consent of the Senate. The term of office of each member of the Board shall be 2 years. The CAN board also will include ex-officio members representing the National Institutes of Health, the Food and Drug Administration and the Department of Defense, the Department of Veterans Affairs and the National Science Foundation. The CAN board will meet four times each calendar year, with 12 board members and representatives of the ex-officio members present at each meeting. The board will be supported by an executive director and other employees that the Board deems necessary to ensure efficient operation of the CAN.

The Chairman of the CAN shall have authority to enter into an interagency agreement with the Center for Scientific Review at the National Institutes of Health to utilize advisory panels to review applications, and to make recommendations to the CAN.

The increases that have been made in medical research over the past 20–30 years have dramatically improved the survival rates for many diseases—deaths from coronary artery disease declined by 18 percent between 1994 and 2004. Stroke deaths also fell by 24.2 percent during that same time period. The five-years survival rates for Hodgkin's lymphoma have increased from 4 percent in the 1960s to more than 86 percent today. Survival rates for localized breast cancer have increased from 80 percent in the 1950s to 98 percent today. Over the past 25 years, survival rates for prostate cancer have increased from 69 percent to almost 99 percent. So we are seeing real progress. But for many other maladies, the statistics are not so good.

These medical advances do not happen overnight. It takes time and money for research institutions to develop scientists skilled in the latest research techniques and to develop the costly infrastructure where research takes place.

Regrettably, Federal funding for NIH has steadily declined from the $3.8 billion increase provided in 2003—when the 5-year doubling of that agency was completed. Had we provided sustained increases of $3.5 billion per year, plus inflation since 2003, we would have $23 billion more in funding for today. The shortfall due to inflationary costs alone is $5.2 billion. This flagging investment in medical research, many believe, served to discourage bright young investigators from entering this field of study.

The $10 billion for the National Institutes of Health that was included in stimulus package provided an immediate infusion of new research dollars for medical research. While these funds will only make up for a portion of what was lost since 2003, it is a step in the right direction. But much remains to be done. Additional dollars must be found for the 2010 appropriation and beyond.

The $40 billion contained in the legislation that I am introducing today will help to re-energize our investment in medical research, support a new generation of young scientists and invest in the health of our Nation.

The bill also contains a provision which requires the Director of NIH to enforce conflict-of-interest policies, requiring primary investigators with financial interests to provide a detailed report how the grant recipient will manage the investigator's conflict-of-interest.

The legislation also elevates the National Center for Minority Health and Health Disparities to Institute status, a designation that will lead to more resources to address the health status of minority and other medically underserved communities.

While some might argue that at a time when our economy is struggling we cannot afford to invest more in medical research. The fact is that research offers the only hope of saving lives, allowing our citizens to lead longer, more productive lives and saving billions of dollars in health care cost. To those critics I would say we cannot afford not to invest in medical research. This is not simply good social policy; it is good economic policy as well.

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

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

S. 914

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 ''Cures Acceleration Network and National Institutes of Health Reauthorization Act of 2009''.

SEC. 2. CURES ACCELERATION NETWORK.

(a) DEFINITIONS.—In this section—

(1) the term ''medical product'' means a drug, device, biological product, or product that is a combination of drugs, devices, and biological products;

(2) the terms ''drug'' and ''device'' have the meanings given such terms in section 201 of the Federal Food, Drug, and Cosmetic Act; and

(3) the term ''biological product'' has the meaning given such term in section 351 of the Public Health Service Act.

(b) ESTABLISHMENT OF THE CURES ACCELERATION NETWORK.—There is established an independent agency to be known as the Cures Acceleration Network (referred to in this section as ''CAN''), which shall—

(1) be under the direction of a CAN Review Board (referred to in this section as the ''Board''), described in subsection (d); and

(2) award grants and contracts to eligible entities, as described in subsection (e), to accelerate the development of cures and treatments of diseases, including through the development of medical products and behavioral therapies.

(c) FUNCTIONS.—The functions of the CAN are to—

(1) identify and promote revolutionary advances in basic research, translating scientific discoveries from bench to bedside;

(2) award grants and contracts to eligible entities;

(3) provide the resources through grants and contracts necessary for independent investigators, research organizations, biotechnology companies, academic research institutions, and other entities to develop medical products for the treatment and cure of diseases and disorders;

(4) reduce the barriers between laboratory discoveries and clinical trials for new therapies;

(5) facilitate priority review in the Food and Drug Administration for the medical products funded by the CAN; and

(6) accept donations, bequests, and gifts to the CAN.

(d) CAN BOARD.—

(1) ESTABLISHMENT.—There is established a Cures Acceleration Network Review Board (referred to in this section as the ''Board''), which shall direct the activities of the Cures Acceleration Network.

(2) MEMBERSHIP.—

(A) IN GENERAL.—

(i) APPOINTMENT.—The Board shall be comprised of 24 members who are appointed by the President and who serve at the pleasure of the President.

(ii) CHAIRPERSON AND VICE CHAIRPERSON.—The President, by and with the advice and consent of the Senate, shall designate, from among the 24 members appointed under clause (i), one Chairperson of the Board (referred to in this section as the ''Chairperson'') and one Vice Chairperson.

(B) TERMS.—

(i) IN GENERAL.—Each member shall be appointed to serve a 4-year term, except that any member appointed to fill a vacancy occurring prior to the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of such term.

(ii) CONSECUTIVE APPOINTMENTS; MAXIMUM TERMS.—A member may be appointed to serve not more than 3 terms on the Board, and may not serve more than 2 such terms consecutively.

(C) QUALIFICATIONS.—

(i) IN GENERAL.—The President shall appoint individuals to the Board based solely upon the individual's established record of distinguished service in one of the areas of expertise described in clause (ii). Each individual appointed to the Board shall be of distinguished achievement and have a broad range of disciplinary interests.

(ii) EXPERTISE.—The President shall select individuals based upon the following requirements:

(I) For each of the fields of—

(aa) basic research;

(bb) medicine;

(cc) biopharmaceuticals;

(dd) discovery and delivery of medical products;

(ee) bioinformatics and gene therapy;

(ff) medical instrumentation; and

(gg) regulatory review and approval of medical products,

the President shall select at least 1 individual who is eminent in such fields.

(II) At least 4 individuals shall be recognized leaders in professional venture capital or private equity organizations and have demonstrated experience in private equity investing.

(III) At least 8 individuals shall represent disease advocacy organizations.

(3) EX-OFFICIO MEMBERS.—

(A) APPOINTMENT.—In addition to the 24 Board members described in paragraph (2), the President shall appoint as ex-officio members of the Board—

(i) a representative of the National Institutes of Health, recommended by the Secretary of the Department of Health and Human Services;

(ii) a representative of the Office of the Assistant Secretary of Defense for Health Affairs, recommended by the Secretary of Defense;

(iii) a representative of the Office of the Under Secretary for Health for the Veterans Health Administration, recommended by the Secretary of Veterans Affairs;

(iv) a representative of the National Science Foundation, recommended by the Chair of the National Science Board; and

(v) a representative of the Food and Drug Administration, recommended by the Commissioner of Food and Drugs.

(B) TERMS.—Each ex-officio member shall serve a 3-year term on the Board, except that the Chairperson may adjust the terms of the initial ex-officio members in order to provide for a staggered term of appointment for all such members.

(4) RESPONSIBILITIES OF THE BOARD.—The Board shall—

(A) advise the Chairperson with respect to policies, programs, and procedures for carrying out the Chairperson's duties; and

(B) review applications for grants and contracts under subsection (e) and make recommendations to the Chairperson.

(5) AUTHORITY OF THE CHAIRPERSON.—The Chairperson may—

(A) prescribe regulations regarding the manner in which the Chairperson's duties shall be carried out, as the Chairperson determines necessary;

(B) appoint employees, subject to civil service laws, as necessary to carry out the Chairperson's functions;

(C) define the duties, and supervise and direct the activities, of any employees appointed under subparagraph (B);

(D) use experts and consultants, including a panel of experts who may be employed as authorized by section 3109 of title 5, United States Code;

(E) accept and utilize the services of voluntary and uncompensated personnel and reimburse such personnel for travel expenses, as described in paragraph (7)(B);

(F) make advance, progress, or other payments without regard to section 3324 of title 31, United States Code;

(G) rent office space in the District of Columbia for use by the CAN;

(H) enter into agreements with other Federal agencies to carry out oversight of the grant program under subsection (e), which agreements may include provisions for financial reimbursement for the oversight provided by such agencies; and

(I) make other necessary expenditures.

(6) MEETINGS.—

(A) IN GENERAL.—The Board shall meet 4 times per calendar year, at the call of the Chairperson.

(B) QUORUM; REQUIREMENTS; LIMITATIONS.—

(i) QUORUM.—A quorum shall consist of a total of 13 members of the Board, excluding ex-officio members, with diverse representation as described in clause (iv).

(ii) CHAIRPERSON OR VICE CHAIRPERSON.—Each meeting of the Board shall be attended by either the Chairperson or the Vice Chairperson.

(iii) LIMITATION.—No member or ex-officio member of the Board may attend more than 2 meetings of the Board each calendar year with the exceptions of the Chairperson and Vice Chairperson, who may attend all such meetings.

(iv) DIVERSE REPRESENTATION.—At each meeting of the Board, there shall be not less than one scientist, one representative of a disease advocacy organization, and one representative of a professional venture capital or private equity organization.

(7) COMPENSATION AND TRAVEL EXPENSES.—

(A) COMPENSATION.—Members shall receive compensation at a rate to be fixed by the Chairperson but not to exceed a rate equal to the daily equivalent of the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day (including travel time) during which the member is engaged in the performance of the duties of the Board. All members of the Board who are officers or employees of the Untied States shall serve without compensation in addition to that received for their services as officers or employees of the United States.

(B) TRAVEL EXPENSES.—Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for persons employed intermittently by the Federal Government under section 5703(b) of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Board.

(e) GRANT PROGRAM.—

(1) GRANTS AND CONTRACTS.—The Chairperson shall, through the Board of the CAN, award grants and contracts to eligible entities to assist such entities in carrying out projects described in paragraph (3).

(2) AWARD PROCESS.—The Chairperson of the Board may award a grant or contract under this subsection to an eligible entity only upon the approval of a majority of a quorum of the Board.

(3) USE OF FUNDS.—Funds awarded under this subsection shall be used—

(A) to accelerate the development of cures and treatments, including through the development of medical products, behavioral therapies, and biomarkers that demonstrate the safety or effectiveness of medical products; or

(B) to help the award recipient establish protocols that comply with Food and Drug

Administration standards and otherwise permit the recipient to meet regulatory requirements at all stages of development, manufacturing, review, approval, and safety surveillance of a medical product.

(4) ELIGIBLE ENTITIES.—To receive a grant or contract under this subsection, an entity shall—

(A) be—

(i) an individual;

(ii) a group of individuals; or

(iii) a public or private entity, which may include a private or public research institution, an institution of higher education, a medical center, a biotechnology company, a pharmaceutical company, a disease advocacy organization, a patient advocacy organization, or an academic research institution;

(B) submit an application containing—

(i) a detailed description of the project for which the entity seeks such grant or contract;

(ii) a timetable for such project;

(iii) an assurance that the entity will submit—

(I) interim reports describing the entity's—

(aa) progress in carrying out the project; and

(bb) compliance with all provisions of this section and conditions of receipt of such grant or contract; and

(II) a final report at the conclusion of the grant period, describing the outcomes of the project; and

(iv) a description of the protocols the entity will follow to comply with Food and Drug Administration standards and regulatory requirements at all stages of development, manufacturing, review, approval, and safety surveillance of a medical product; and

(C) provide such additional information as the Chairperson may require.

(5) STUDY SECTIONS OF THE CENTER FOR SCIENTIFIC REVIEW.—

(A) IN GENERAL.—The Chairperson may enter into an interagency agreement with the Center for Scientific Review within the National Institutes of Health to use the study sections of such Center to review applications submitted under paragraphs (4)(B) and additional information submitted under (4)(C) and to make recommendations to the Board. The Chairperson shall promulgate regulations and procedures to—

(i) ensure that each study section reviewing applications is composed of diverse members, as described in subparagraph (B);

(ii) require such study sections to create written records summarizing—

(I) all meetings and discussions of the study section; and

(II) the recommendations made by such study section to the Board; and

(iii) make the records described in clause (ii) available to the public in a manner that protects the privacy of applicants and panel members and any proprietary information from applicants.

(B) MEMBERSHIP.—The Chairperson shall ensure that the study sections of the Center for Scientific Review that review applications submitted under this subsection are selected solely on the basis of established records of distinguished service and include—

(i) for each of the fields of—

(I) basic research;

(II) medicine;

(III) biopharmaceuticals;

(IV) discovery and delivery of medical products;

(V) bioinformatics and gene therapy; and

(VI) medical instrumentation,

at least 2 individuals with expertise in such fields;

(ii) at least 3 representatives of professional venture capital or private equity organizations with demonstrated experience in private equity investing; and

(iii) at least 3 representatives of disease advocacy organizations.

(C) FINANCIAL COMPENSATION.—Any agreement under subparagraph (A) shall include an arrangement whereby the Chairperson reimburses the Center for Scientific Review for the services provided under such subparagraph.

(6) AWARDS.—

(A) THE CURES ACCELERATION PARTNERSHIP AWARDS.—

(i) INITIAL AWARD AMOUNT.—Each award under this subparagraph shall be not more than $15,000,000 per project for the first fiscal year for which the project is funded, which shall be payable in one payment, except that the Chairperson of the Board may increase the award amount for an eligible entity if the Board so determines by a majority vote.

(ii) FUNDING IN SUBSEQUENT FISCAL YEARS.—An eligible entity receiving an award under clause (i) may apply for additional funding for such project by submitting to the Board the information required under subparagraphs (B) and (C) of paragraph (4). The Chairperson may fund a project of such eligible entity in an amount not to exceed $15,000,000 for a fiscal year subsequent to the initial award under clause (i) if the Board so determines by majority vote.

(iii) MATCHING FUNDS.—As a condition for receiving a grant or contract under this subparagraph, an eligible entity shall contribute to the project non-Federal funds in the amount of $1 for every $3 awarded under clauses (i) and (ii), except that the Chairperson may waive or modify such matching requirement by a majority vote of the Board.

(B) THE CURES ACCELERATION GRANT AWARDS.—

(i) INITIAL AWARD AMOUNT.—Each award under this subparagraph shall be not more than $15,000,000 per project for the first fiscal year for which the project is funded, which shall be payable in one payment, except that the Chairperson of the Board may increase the award amount for an eligible entity if the Board so determines by a majority vote.

(ii) FUNDING IN SUBSEQUENT FISCAL YEARS.—An eligible entity receiving an award under clause (i) may apply for additional funding for such project by submitting to the Board the information required under subparagraphs (B) and (C) of paragraph (4). The Chairperson may fund a project of such eligible entity in an amount not to exceed $15,000,000 for a fiscal year subsequent to the initial award under clause (i) if the Board so determines by majority vote.

(7) SUSPENSION OF AWARDS FOR DEFAULTS, NONCOMPLIANCE WITH PROVISIONS AND PLANS, AND DIVERSION OF FUNDS; REPAYMENT OF FUNDS.—The Chairperson may suspend the award to any entity upon noncompliance by such entity with provisions and plans under this section or diversion of funds.

(8) AUDITS.—The Chairperson may enter into agreements with other entities to conduct periodic audits of the projects funded by grants or contracts awarded under this subsection.

(9) CLOSEOUT PROCEDURES.—At the end of a grant or contract period, a recipient shall follow the closeout procedures under section 74.71 of title 45, Code of Federal Regulations (or any successor regulation).

(f) STAFF.—The CAN may employ such officers and employees (including experts and consultants), appointed by the Chairperson, as may be necessary to enable the CAN to carry out its functions under this section, and may employ and fix the compensation of such officers and employees.

(g) GIFTS, BEQUESTS, AND DEVISES.—

(1) IN GENERAL.—The CAN may accept donations, bequests, and devises, with or without conditions, and transfers for tax purposes, for the purpose of aiding or facilitating the work of the CAN subject to the following:

(A) In any case in which money or other property is donated, bequeathed, or devised to the CAN without designation for the benefit of which such property is intended, and without condition or restriction other than that such property be used for the purposes of the CAN, such property shall be deemed to have been donated, bequeathed, or devised to the CAN and the Chairperson shall have authority to receive such property.

(B) In any case in which any money or other property is donated, bequeathed, or devised to the CAN with a condition or restriction, such property shall be deemed to have been donated, bequeathed, or devised to the CAN whose function it is to carry out the purpose or purposes described, or referred to, by the terms of such condition or restriction, and the Chairperson shall have authority to receive such property.

(C) For the purposes of subparagraph (B), if one or more of the purposes of such a condition or restriction is covered by the functions of the CAN, or if some of the purposes of such a condition or restriction are covered by the CAN, the Board shall determine an equitable manner for distribution by the CAN of the property so donated, bequeathed, or devised.

(D) For the purpose of Federal income tax, gift tax, and estate tax laws, any money or other property donated, bequeathed, or devised to the Chairperson pursuant to authority derived under this subsection shall be deemed to have been donated, bequeathed, or devised to, or for the use of, the United States.

(h) CONFLICTS OF INTEREST.—

(1) IN GENERAL.—The Chairperson shall develop and enforce conflict of interest policies for the CAN and shall respond in a timely manner when such policies have been violated by a recipient of funds provided under a grant or contract awarded under this section.

(2) INFORMATION.—

(A) IN GENERAL.—In the case in which the principal investigator for a recipient described under subparagraph (B) has a conflict of interest, the Chairperson shall require the recipient to provide to the Chairperson the following information:

(i) The degree of the primary investigator's financial interest, estimated to the nearest $1,000.

(ii) A detailed report explaining how the recipient will manage the primary investigator's conflict of interest.

(B) RECIPIENT.—A recipient described in this subparagraph is a recipient—

(i) of a grant or contract awarded under subsection (e); and

(ii) that receives more than $250,000 under such grant or contract.

(i) AUTHORIZATION OF APPROPRIATIONS.—For purposes of carrying out this section, there are authorized to be appropriated—

(1) for fiscal year 2010, $1,000,000,000 for awards described under subsection (e)(6)(A), including associated administrative costs;

(2) for fiscal year 2010, $1,000,000,000 for awards described under subsection (e)(6)(B), including associated administrative costs; and

(3) such sums as may be necessary for subsequent fiscal years.

SEC. 3. ORGANIZATION OF NATIONAL INSTITUTES OF HEALTH.

(a) REDESIGNATION OF CENTER ON MINORITY HEALTH AND HEALTH DISPARITIES.—Title IV of the Public Health Service Act (42 U.S.C. 281 et seq.) is amended—

(1) by redesignating subpart 6 of part E as subpart 20;

(2) by transferring subpart 20, as so redesignated, to part C of such title IV;

(3) by inserting subpart 20, as so redesignated, after subpart 19 of such part C; and

(4) in subpart 20, as so redesignated—

(A) by redesignating sections 485E through 485H as sections 464z-3 through 464z-6, respectively;

(B) by striking ''National Center on Minority Health and Health Disparities'' each place such term appears and inserting ''National Institute on Minority Health and Health Disparities''; and

(C) by striking ''Center'' each place such term appears and inserting ''Institute''.

(b) PURPOSE OF INSTITUTE.—Subsection (h) of section 464z-3 of the Public Health Service Act, as so redesignated, is amended—

(1) in paragraph (1), by striking ''research endowments at centers of excellence under section 736.'' and inserting the following: ''research endowments—

''(1) at centers of excellence under section 736; and

''(2) at centers of excellence under section 464z-4.''; and

(2) in paragraph (2)(A), by striking ''average'' and inserting ''median''.

(c) TECHNICAL AMENDMENT.—Section 401(b)(24) of the Public Health Service Act (42 U.S.C. 281(b)(24)) is amended by striking ''Center'' and inserting ''Institute''.

(d) CONFORMING AMENDMENT.—Subsection (d)(1) of section 903 of the Public Health Service Act (42 U.S.C. 299a-1(d)(1)) is amended by striking ''section 485E'' and inserting ''section 464z-3''.

SEC. 4. CONFLICTS OF INTEREST.

Section 402 of the Public Health Service Act (42 U.S.C. 282) is amended by adding at the end the following:

''(m) ENFORCEMENT OF CONFLICT OF INTEREST POLICIES.—

''(1) IN GENERAL.—The Director shall develop and enforce the conflict of interest policies for the National Institutes of Health and shall respond in a timely manner when such policies have been violated by a recipient of funds provided under a grant or contract awarded under this title.

''(2) INFORMATION.—

''(A) IN GENERAL.—In the case in which the principal investigator for a recipient described under subparagraph (B) has a conflict of interest, the Director shall require the recipient to provide to the Director the following information:

''(i) The degree of the primary investigator's financial interest, estimated to the nearest $1,000.

''(ii) A detailed report explaining how the recipient will manage the primary investigator's conflict of interest.

''(B) RECIPIENT.—A recipient described in this subparagraph is a recipient—

''(i) of a grant or contract awarded under this title; and

''(ii) that receives more than $250,000 under such grant or contract.''.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

(a) AUTHORIZATION OF APPROPRIATIONS.—Section 402A of the Public Health Service Act (42 U.S.C. 282a) is amended by striking paragraphs (1) through (3) of subsection (a) and inserting the following:

''(1) $40,000,000,000 for fiscal year 2010; and

''(2) such sums as may be necessary for each of fiscal years 2011 and 2012.''.

(b) OFFICE OF THE DIRECTOR.—Subparagraph (b) of section 402A of the Public Health Service Act (42 U.S.C. 282a(b)) is amended by striking ''2007 through 2009'' and inserting ''2010 through 2012''.

SUPPORTERS

Autism Speaks, Association of Minority Health Professions Schools, Morehouse School of Medicine, Meharry Medical College, Charles Drew University of Medicine and Science, Cure Alzheimer's Fund, American Thoracic Society, Scleroderma Foundation, NephCure Foundation, National Marfan Foundation, Crohn's and Colitis Foundation of America, Pulmonary Hypertension Association, Biotechnology Industry Organization, Melanoma Research Foundation, Alzheimer's Association, Medical Library Association, Association of Academic Health Sciences Libraries, American Lung Association, Lupus Research Institute, S.L.E. Lupus Foundation, Friends of Cancer Research, College on Problems of Drug Dependence, Parkinson's Action Network.

By Mr. GREGG:

S. 917. A bill provide assistance to Pakistan under certain conditions, and for other purposes; to the Committee on Foreign Relations.

Mr. GREGG. Mr. President, I rise today to introduce legislation that provides the President with extraordinary, but critical authority under section 451 of the Foreign Assistance Act of 1961 with respect to assistance for Pakistan.

Specifically, the bill allows the President to reprogram up to $500,000,000 of previously appropriated foreign operations funds for assistance for Pakistan if the President determines that it is in the vital national security interests of the U.S. to do so.

The President must still report promptly to Congress on the exercise of this authority, and it is my expectation—although not legally binding—that reprogrammed funds will be reimbursed in subsequent annual or supplemental appropriations bills.

Extended until September 30, 2010, this authority is required because of the increasingly dire situation in Pakistan and alarming news reports of territorial gains by extremists. While I do not pretend to have the answers to Pakistan's myriad challenges, I do know that the administration lacks the necessary authority to reprogram significant funds to respond to further political and economic deterioration in that country. Should the government of Pakistani President Zardari collapse, the administration will need maximum flexibility in its response.

I can anticipate some may have a knee jerk reaction to the provision of such extraordinary authority. In response, I would remind my colleagues that regardless of their opinions of Pakistan's messy political situation, events in Pakistan directly impact Afghanistan—and our troops on the ground there.

Of course, this is in addition to the impact that destabilization would have on Pakistan's nuclear complex, specifically the combination of dozens of nuclear weapons, untested security systems, and a surplus of Islamic militants in the area. These issues are at the forefront of our security interests in the region and would exacerbate exponentially the impact of destabilization.

It might interest my colleagues to know that current law limits section 451 reprogram authority to $25,000,000. In contrast, the supplemental budget request seeks $4,000,000,000 in special transfer authority for the Department of Defense to meet emerging requirements. Surely, the State Department should also have increased flexibility to react promptly to the economic and security needs of Pakistan should the worst case scenario transpire.

I urge the relevant Committee to consider and act upon this legislation quickly.

By Mr. AKAKA:

S. 919. A bill to amend section 1154 of title 58, United States Code, to clarify the additional requirements for consideration to be afforded time, place, and circumstances of service in determinations regarding service-connected disabilities; to the Committee on Veterans' Affairs.

Mr. AKAKA. Mr. President, I am today introducing the proposed Clarification of Characteristics of Combat Service Act of 2009. This legislation is designed to address concerns which have been noted during the Committee's oversight visits to VA regional offices. From the review of claims folders as part of ongoing oversight, Committee staff has noted that VA adjudicators often fail to factor in the existence of common occurrences when considering claims from combat veterans because there is no formal evidence on the matters in question in the claimant's official military records.

When common hazards exist in particular areas where our armed forces have or are serving, a means must be established to determine whether a particular veteran's claim of exposure to such hazard or matter is consistent with the circumstances of service in that area, even without evidence in individual official records. This proposed bill would establish a mechanism by requiring VA to promulgate regulations that would include standards that VA adjudicators would use for evaluating the consistency between lay evidence and claimed matters, such as exposure to factors common to servicemembers serving in particular combat areas.

This proposed bill is intended to result in recognition by VA that, where there is evidence of common events, a veteran's testimony, if consistent with other evidence, would be accepted without requiring specific, formal evidence of individual exposure to the event. By law, lay testimony is currently recognized in claims where a veteran served in a military unit which participated in combat. While this bill is not intended to provide a presumption of service-connection for any particular disability, it should improve the accurate adjudication of claims in those cases where a veteran served in an area where certain events or exposures are widespread.

For example, there is widespread agreement that those who have served in Iraq since the start of the conflict there have been exposed to improvised explosive devices—IEDs. However,

based on Committee oversight, it appears that it often happens that, when a veteran applies for compensation for disabilities related to IED exposure, such as tinnitus, the claim may be denied if the veteran's service medical record does not show treatment for tinnitus in service or otherwise documents exposure to an IED. Since it would be highly unusual to find documentation of treatment where a veteran in a combat zone has consulted with medical personnel for a relatively minor condition, such as exposure to an IED which did not cause acute observable injury, the formal records would not be of use to the claimant. The regulations required by the legislation I am introducing would likely include provision for conceding exposure to an IED in claims brought by veterans who served in Iraq.

Another example of the problems that the legislation is designed to address involves claims from Korean war veterans, many of whom were exposed to extreme cold, but whose records may not have documentation of treatment for a cold injury or information on the actual temperature to which they were exposed. I would anticipate that the regulations required by this legislation would provide for VA to concede exposure to subfreezing temperatures in such cases if consistent with the location where the veteran served.

I expect that this measure should speed the processing by claims, by not requiring each veteran to individually establish by official government records, which often do not document individual participation, exposure to one or more events which are well established as circumstances involving the place and type of the veteran's service.

In closing, I note that this legislation has been developed in consultation with VA and with a variety of individuals and groups interested in VA claims but I do not view it as a final approach. I look forward to working with my colleagues on the Committee and in the Senate, as well as with those with an interest in this issue, to improve this bill so that combat veterans of the current conflicts and of earlier conflicts who allege exposure to well-recognized events will not be burdened by requirements of acquiring official evidence of individual participation in such events. This should help veterans receive the benefits they deserve in a timely manner. I urge support for this legislation.

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. 919

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 ''Clarification of Characteristics of Combat Service Act of 2009''.

SEC. 2. CLARIFICATION OF ADDITIONAL REQUIREMENTS FOR CONSIDERATION TO BE AFFORDED TIME, PLACE, AND CIRCUMSTANCES OF SERVICE IN DETERMINATIONS REGARDING SERVICE-CONNECTED DISABILITIES.

Subsection (a) of section 1154 of title 38, United States Code, is amended to read as follows:

''(a)(1) The Secretary shall include in the regulations pertaining to service-connection of disabilities the following:

''(A) Additional provisions in effect requiring that in each case where a veteran is seeking service-connection for any disability due consideration shall be given to the places, types, and circumstances of such veteran's service as shown by such veteran's service record, the official history of each organization in which such veteran served, such veteran's medical records, and all pertinent medical and lay evidence.

''(B) Additional provisions specifying that, in the case of a veteran who served in a particular combat zone, the Secretary shall accept credible lay or other evidence as sufficient proof that the veteran encountered an event that the Secretary specifies in such regulations as associated with service in particular locations where the veteran served or in particular circumstances under which the veteran served in such combat zone.

''(C) The provisions required by section 5 of the Veterans' Dioxin and Radiation Exposure Compensation Standards Act (Public Law 98–542; 98 Stat. 2727).

''(2) In paragraph (1)(B), the term 'combat zone' means a combat zone for purposes of section 112 of the Internal Revenue Code of 1986 or a predecessor provision of law.''.

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

S. 920. A bill to amend section 11317 of title 40, United States Code, to improve the transparency of the status of information technology investments, to require greater accountability for cost overruns on Federal information technology investment projects, to improve the processes agencies implement to manage information technology investments, to reward excellence in information technology acquisition, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

Mr. CARPER. Mr. President, I rise today to introduce two bills, S. 920 and S. 921, that I believe could represent the most sweeping reforms of government information technology management reform we've considered in some time.

I would like to start by addressing the IT Investment Oversight and Waste Prevention Act.

Every year, agencies spend billions of dollars on IT investments that they believe will increase productivity, reduce costs, or improve customer service. But agencies often fail to properly plan and manage their investments. Rather, nearly one third of all Federal IT investments are considered by OMB to be ''poorly planned.'' Many of these investments will be delivered over budget, behind schedule, and not performing up to agencies' original expectations.

Some might say that we just shouldn't make these kinds of investments. But many of them are critical to agency missions.

My colleagues and I on the Homeland Security and Governmental Affairs Committee's Subcommittee on Federal Financial Management, which I chair, have held four hearings on the issue of troubled IT investments now, including one today. And what we've learned is that some agencies can't keep the expected cost of their investments down or deliver them on time as promised. Nor do these agencies, in many cases, have qualified IT experts they can turn to before a project spirals out of control. The bill I have put forward today along with a number of my colleagues addresses these issues.

Our bill starts by requiring the Office of Management and Budget to increase the transparency of funded IT investments on a public website. OMB created such a website, known as VUE-IT, this past July following one of our subcommittee hearings. Our bill would ensure that VUE-IT or whatever similar site the new Obama team creates has the cost, schedule, and performance necessary for Congress and the general public to know if a project is a success or should be scrapped.

Our bill also requires that agency plans for new IT systems must contain a clear business case and provide complete and accurate information before the OMB approves the investments. Although this sounds like a simple concept, it doesn't always happen. And OMB has historically been unwilling to turn down an agency IT request.

To correct this, our bill also empowers OMB and agency Chief Information Officers to take action if they realize a project isn't going as planned, before it spirals out of control. This action could be the assignment of highly-trained IT experts who could help bring projects back on track.

Lastly, our bill recognizes that there are a lot of innovative and hard-working federal employees that deserve recognition for the work they do in information technology. Our bill requires the Office of Personnel Management to provide agencies guidance on programs that can be set up to reward employees for their excellence.

Now, I would like to discuss my next bill titled the United States Information and Communications Enhancement Act of 2009.

Everyday, massive amounts of information are transmitted across the global information infrastructure. Some of this information is routine email between friends and family. Much of it, however, consists of highly sensitive military information, however, or commercial secrets.

As all of us can attest to, increasing global interconnectivity has greatly increased our productivity and ability to communicate. However, it has also increased our responsibility to make sure this information is protected.

The Federal Government stores within its databases some of our nation's most critical military, economic, and commercial secrets. Great harm could be caused if it were to fall into the

wrong hands. Knowing this, hackers, criminal organizations, and even other countries are spending a good deal of money and time trying to access it.

In fact, just last week we learned that someone had gone online and stolen our military's most advanced jet fighter plans with the stroke of a button. The cost to the American taxpayer for this single incident is approximately $300 billion worth of research and development, and an incalculable amount if the information were to ever be used against us.

Unfortunately, many agencies have not done as much as they should be doing to prevent these cyber intrusions. Instead they have been led to believe that producing plans about cyber security is equivalent to actually monitoring and protecting their networks. My bill will correct this.

First, my bill recognizes that there needs to be a coordinating office to oversee the multiple agencies that have a hand in cyber space. Today, the NSA and the Departments of Homeland Security and Defense all have different roles when it comes to securing cyber networks in the federal government and the private sector. Their efforts are largely uncoordinated and ineffective. This bill creates a White House office with a director confirmed by the Senate whose major responsibility would be to rectify this situation

My bill also ensures that agencies are spending scarce resources effectively. Instead of agencies wasting precious resources producing security plans that are outdated as soon they are printed, my bill requires agencies to continuously monitor their networks for cyber intrusions and malicious activities, take steps to address their vulnerabilities, and then regularly test whether the steps they are taking to secure their networks are effective.

My bill also requires the General Service Administration to harness the significant purchasing power of the federal government to purchase more secure hardware and software. This is the model the Air Force used a few years ago with Microsoft and it led to a savings of approximately $98 million in one year and an enhanced security posture. This is a successful model that we should continue throughout the federal government.

Lastly, my bill recognizes that the Department of Homeland Security has taken the lead among civilian agencies in protecting the perimeter of the federal government but lacks some of the necessary authority and technical people necessary to realize a more secure civilian cyber space. Therefore, our bill will require agencies to develop policy and guidance for coordinating with US-CERT and give the Director of US-CERT the ability to hire the personnel needed to defend our national security.

I look forward to working with my colleagues to get these important and necessary reforms enacted before it's too late. I think everyone can agree that computers, the Internet, and cutting-edge technology have greatly benefited our government and our society. But we also need to recognize that it has greatly increased the threats we face on a daily basis.

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 placed in the RECORD, as follows:

S. 920

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 ''Information Technology (IT) Investment Oversight Enhancement and Waste Prevention Act of 2009''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) The effective deployment of information technology can make the Federal Government more efficient, effective, and transparent.

(2) Historically, the Federal Government has struggled to properly plan, manage, and deliver information technology investments on time, on budget, and performing as planned.

(3) The Office of Management and Budget has made significant progress overseeing information technology investments made by Federal agencies but continues to struggle to ensure that such investments meet cost, schedule, and performance expectations.

(4) Congress has limited knowledge of the actual cost, schedule, and performance of agency information technology investments and has difficulty providing the necessary oversight.

(5) In July 2008, an official of the Government Accountability Office testified before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security of the Committee on Homeland Security and Governmental Affairs of the Senate, stating that—

(A) agencies self-report inaccurate and unreliable project management data to the Office of Management and Budget and Congress; and

(B) the Office of Management and Budget should establish a mechanism that would provide real-time project management information and force agencies to improve the accuracy and reliability of the information provided.

SEC. 3. REAL-TIME TRANSPARENCY OF IT INVESTMENT PROJECTS.

Section 11302(c)(1) of title 40, United States Code, is amended by striking the period at the end and inserting the following: '', including establishing a Website, updating the Website on a quarterly basis, and including on the Website, not later than 90 days after the date of the enactment of the Information Technology (IT) Investment Oversight Enhancement and Waste Prevention Act of 2009—

''(1) the cost, schedule, and performance of all major information technology investments using earned-value management data based on the ANSI–EIA–748–B standard;

''(2) accurate quarterly information since the commencement of the project;

''(3) a graphical depiction of trend information since the commencement of the project;

''(4) a clear delineation of investments that have experienced cost, schedule, or performance variance greater than 10 percent over the life cycle of the investment;

''(5) an explanation of the reasons the investment deviated from the benchmark established at the commencement of the project; and

''(6) the number of times investments were rebaselined and the dates on which such rebaselines occurred.''.

SEC. 4. IT INVESTMENT PROJECTS.

(a) SIGNIFICANT AND GROSS DEVIATIONS.—Section 11317 of title 40, United States Code, is amended to read as follows:

''SEC. 11317. SIGNIFICANT AND GROSS DEVIATIONS.

''(a) DEFINITIONS.—In this subchapter:

''(1) AGENCY HEAD.—The term 'Agency Head' means the head of the Federal agency that is primarily responsible for the IT investment project under review.

''(2) ANSI EIA–748–B STANDARD.—The term 'ANSI EIA–748–B Standard' means the measurement tool jointly developed by the American National Standards Institute and the Electronic Industries Alliance to analyze Earned Value Management systems.

''(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Committee on Oversight and Government Reform of the House of Representatives;

''(C) the Committee on Appropriations of the Senate;

''(D) the Committee on Appropriations of the House of Representatives; and

''(E) any other relevant congressional committee with jurisdiction over an agency required to take action under this section.

''(4) CHIEF INFORMATION OFFICER.—The term 'Chief Information Officer' means the Chief Information Officer designated under section 3506(a)(2) of title 44 of the Federal agency that is primarily responsible for the IT investment project under review.

''(5) CORE IT INVESTMENT PROJECT.—The terms 'core IT investment project' and 'core project' mean a mission critical IT investment project designated as such by the Chief Information Officer, with approval by the Agency Head under subsection (b).

''(6) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget.

''(7) EARNED VALUE MANAGEMENT.—The term 'Earned Value Management' means the cost, performance, and schedule data used to determine project status and developed in accordance with the ANSI EIA–748-B Standard.

''(8) GROSSLY DEVIATED.—The term 'grossly deviated' means cost, schedule, or performance variance that is at least 40 percent from the Original Baseline.

''(9) INDEPENDENT GOVERNMENT COST ESTIMATE.—The term 'independent government cost estimate' means a pragmatic and neutral analysis, assessment, and quantification of all costs and risks associated with the acquisition of an IT investment project, which—

''(A) is based on programmatic and technical specifications provided by the office within the agency with primary responsibility for the development, procurement, and delivery of the project;

''(B) is formulated and provided by an entity other than the office within the agency with primary responsibility for the development, procurement, and delivery of the project;

''(C) contains sufficient detail to inform the selection of an Earned Value Management baseline benchmark measure under the ANSI EIA–748-B standard; and

''(D) accounts for the full life cycle cost plus associated operations and maintenance expenses over the usable life of the project's deliverables.

''(10) IT INVESTMENT PROJECT.—The terms 'IT investment project' and 'project' mean an information technology system or information technology acquisition that—

''(A) requires special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization;

''(B) is for financial management and obligates more than $500,000 annually;

''(C) has significant program or policy implications;

''(D) has high executive visibility;

''(E) has high development, operating, or maintenance costs;

''(F) is funded through other than direct appropriations; or

''(G) is defined as major by the agency's capital planning and investment control process.

''(11) LIFE CYCLE COST.—The term 'life cycle cost' means the total cost of an IT investment project for planning, research and development, modernization, enhancement, operation, and maintenance.

''(12) ORIGINAL BASELINE.—

''(A) IN GENERAL.—Except as provided under subparagraph (B), the term 'Original Baseline' means the ANSI EIA–748–B Standard-compliant Earned Value Management benchmark established at the commencement of an IT investment project.

''(B) GROSSLY DEVIATED PROJECT.—If an IT investment project grossly deviates from its Original Baseline (as defined in subparagraph (A)), the term 'Original Baseline' means the ANSI EIA–748–B Standard-compliant Earned Value Management benchmark established under subsection (e)(3)(C).

''(13) SIGNIFICANTLY DEVIATED.—The term 'significantly deviated' means Earned Value Management variance that is at least 20 percent from the Original Baseline.

''(b) CORE IT INVESTMENT PROJECTS DESIGNATION.—Each Chief Information Officer, with approval by the Agency Head, shall—

''(1) identify the major IT investments that are the most critical to the agency; and

''(2) designate any project as a 'core IT investment project' or a 'core project', upon determining that the project is a mission critical IT investment project that—

''(A) represents a significant high dollar value relative to the average IT investment project in the agency's portfolio;

''(B) delivers a capability critical to the successful completion of the agency mission, or a portion of such mission;

''(C) incorporates unproven or previously undeveloped technology to meet primary project technical requirements; or

''(D) would have a significant negative impact on the successful completion of the agency mission if the project experienced significant cost, schedule, or performance deviations.

''(c) COST, SCHEDULE, AND PERFORMANCE REPORTS.—

''(1) QUARTERLY REPORTS.—Not later than 14 days after the end of each fiscal quarter, the project manager designated by the Agency Head for an IT investment project shall submit a written report to the Chief Information Officer that includes, as of the last day of the applicable quarter—

''(A) a description of the cost, schedule, and performance of all projects under the project manager's supervision;

''(B) the original and current project cost, schedule, and performance benchmarks for each project under the project manager's supervision;

''(C) the quarterly and cumulative cost, schedule, and performance variance related to each IT investment project under the project manager's supervision since the commencement of the project;

''(D) for each project under the project manager's supervision, any known, expected, or anticipated changes to project schedule milestones or project performance benchmarks included as part of the original or current baseline description;

''(E) the current cost, schedule, and performance status of all projects under supervision that were previously identified as significantly deviated or grossly deviated; and

''(F) any corrective actions taken to address problems discovered under subparagraphs (C) through (E).

''(2) INTERIM REPORTS.—If the project manager for an IT investment project determines that there is reasonable cause to believe that an IT investment project has significantly deviated or grossly deviated since the issuance of the latest quarterly report, the project manager shall submit to the Chief Information Officer, not later than 14 days after such determination, a report on the project that includes, as of the date of the report—

''(A) a description of the original and current program cost, schedule, and performance benchmarks;

''(B) the cost, schedule, or performance variance related to the IT investment project since the commencement of the project;

''(C) any known, expected, or anticipated changes to the project schedule milestones or project performance benchmarks included as part of the original or current baseline description;

''(D) the major reasons underlying the significant or gross deviation of the project; and

''(E) a corrective action plan to correct such deviations.

''(d) DETERMINATION OF SIGNIFICANT DEVIATION.—

''(1) CHIEF INFORMATION OFFICER.—Upon receiving a report under subsection (c), the Chief Information Officer shall—

''(A) determine if any IT investment project has significantly deviated; and

''(B) report such determination to the Agency Head.

''(2) CONGRESSIONAL NOTIFICATION.—If the Chief Information Officer determines under paragraph (1) that an IT investment project has significantly deviated and the Agency Head has not issued a report to the appropriate congressional committees of a significant deviation for that project under this section since the project was last required to be rebaselined under this section, the Agency Head shall submit a report to the appropriate congressional committees, the Director, and the Government Accountability Office that includes—

''(A) written notification of such determination;

''(B) the date on which such determination was made;

''(C) the amount of the cost increases and the extent of the schedule delays with respect to such project;

''(D) any requirements that—

''(i) were added subsequent to the original contract; or

''(ii) were originally contracted for, but were changed by deferment or deletion from the original schedule, or were otherwise no longer included in the requirements contracted for;

''(E) an explanation of the differences between—

''(i) the estimate at completion between the project manager, any contractor, and any independent analysis; and

''(ii) the original budget at completion;

''(F) a statement of the reasons underlying the project's significant deviation; and

''(G) a summary of the plan of action to remedy the significant deviation.

''(3) DEADLINE.—

''(A) NOTIFICATION BASED ON QUARTERLY REPORT.—If the determination of significant deviation is based on a report submitted under subsection (c)(1), the Agency Head shall notify Congress and the Director in accordance with paragraph (2) not later than 21 days after the end of the quarter upon which such report is based.

''(B) NOTIFICATION BASED ON INTERIM REPORT.—If the determination of significant deviation is based on a report submitted under subsection (c)(2), the Agency Head shall notify Congress and the Director in accordance with paragraph (2) not later than 21 days after the submission of such report.

''(e) DETERMINATION OF GROSS DEVIATION.—

''(1) CHIEF INFORMATION OFFICER.—Upon receiving a report under subsection (c), the Chief Information Officer shall—

''(A) determine if any IT investment project has grossly deviated; and

''(B) report any such determination to the Agency Head.

''(2) CONGRESSIONAL NOTIFICATION.—If the Chief Information Officer determines under paragraph (1) that an IT investment project has grossly deviated and the Agency Head has not issued a report to the appropriate congressional committees of a gross deviation for that project under this section since the project was last required to be rebaselined under this section, the Agency Head shall submit a report to the appropriate congressional committees, the Director, and the Government Accountability Office that includes—

''(A) written notification of such determination, which—

''(i) identifies the date on which such determination was made; and

''(ii) indicates whether or not the project has been previously reported as a significant or gross deviation by the Chief Information Officer, and the date of any such report;

''(B) incorporations by reference of all prior reports to Congress on the project required under this section;

''(C) updated accounts of the items described in subparagraphs (C) through (G) of subsection (d)(2);

''(D) the original estimate at completion for the project manager, any contractor, and any independent analysis;

''(E) a graphical depiction that shows monthly planned expenditures against actual expenditures since the commencement of the project;

''(F) the amount, if any, of incentive or award fees any contractor has received since the commencement of the contract and the reasons for receiving such incentive or award fees;

''(G) the project manager's estimated cost at completion and estimated completion date for the project if current requirements are not modified;

''(H) the project manager's estimated cost at completion and estimated completion date for the project based on reasonable modification of such requirements;

''(I) an explanation of the most significant occurrence contributing to the variance identified, including cost, schedule, and performance variances, and the effect such occurrence will have on future project costs and program schedule;

''(J) a statement regarding previous or anticipated rebaselining or replanning of the project and the names of the individuals responsible for approval;

''(K) the original life cycle cost of the investment and the expected life cycle cost of the investment expressed in constant base year dollars and in current dollars; and

''(L) a comprehensive plan of action to remedy the gross deviation, and milestones

established to control future cost, schedule, and performance deviations in the future.

''(3) REMEDIAL ACTION.—

''(A) IN GENERAL.—If the Chief Information Officer determines under paragraph (1)(A) that an IT investment project has grossly deviated, the Agency Head, in consultation with the Chief Information Officer and the appropriate project manager, shall develop and implement a remedial action plan that includes—

''(i) a report that—

''(I) describes the primary business case and key functional requirements for the project;

''(II) describes any portions of the project that have technical requirements of sufficient clarity that such portions may be feasibly procured under firm, fixed-price type contract;

''(III) includes a certification by the Agency Head, after consultation with the Chief Information Officer, that all technical and business requirements have been reviewed and validated to ensure alignment with the reported business case;

''(IV) describes any changes to the primary business case or key functional requirements which have occurred since project inception; and

''(V) includes an independent government cost estimate for the project conducted by an entity approved by the Director;

''(ii) an analysis that—

''(I) describes agency business goals that the project was originally designed to address;

''(II) includes a gap analysis of what project deliverables remain in order for the agency to accomplish the business goals referred to in subclause (I);

''(III) identifies the 3 most cost-effective alternative approaches to the project which would achieve the business goals referred to in subclause (I); and

''(IV) includes a cost-benefit analysis, which compares—

''(aa) the completion of the project with the completion of each alternative approach, after factoring in future costs associated with the termination of the project; and

''(bb) the termination of the project without pursuit of alternatives, after factoring in foregone benefits; and

''(iii) a new baseline of the project is established that is consistent with the independent government cost estimate required under clause (i)(V); and

''(iv) the project is designated as a core IT investment project and subjected to the requirements under subsection (f).

''(B) SUBMISSION TO CONGRESS.—The remedial action plan and all corresponding reports, analyses, and actions under this paragraph shall be submitted to the appropriate congressional committees and the Director.

''(C) REPORTING AND ANALYSIS EXEMPTIONS.—

''(i) IN GENERAL.—The Chief Information Officer, in coordination with the Agency Head and the Director, may forego the completion of any element of a report or analysis under clause (i) or (ii) of subparagraph (A) if the Chief Information Officer determines that such element is not relevant to the understanding of the difficulties facing the project or that such element does not further the remedial steps necessary to ensure that the project is completed in a timely and cost-efficient manner.

''(ii) IDENTIFICATION OF REASONS.—The Chief Information Officer shall include the reasons for not including any element referred to in clause (i) in the report submitted to Congress under subparagraph (B).

''(4) DEADLINE AND FUNDING CONTINGENCY.—

''(A) NOTIFICATION AND REMEDIAL ACTION BASED ON QUARTERLY REPORT.—

''(i) IN GENERAL.—If the determination of gross deviation is based on a report submitted under subsection (c)(1), the Agency Head shall—

''(I) not later than 45 days after the end of the quarter upon which such report is based, notify the appropriate congressional committees and the Director in accordance with paragraph (2); and

''(II) not later than 180 days after the end of the quarter upon which such report is based, ensure the completion of remedial action under paragraph (3).

''(ii) FAILURE TO MEET DEADLINES.—If the Agency Head fails to meet the deadline described in clause (i)(II), additional funds may not be obligated to support expenditures associated with the project until the requirements of this subsection have been fulfilled.

''(B) NOTIFICATION AND REMEDIAL ACTION BASED ON INTERIM REPORT.—

''(i) IN GENERAL.—If the determination of gross deviation is based on a report submitted under subsection (c)(2), the Agency Head shall—

''(I) not later than 45 days after the submission of such report, notify the appropriate congressional committees in accordance with paragraph (2); and

''(II) not later than 180 days after the submission of such report, ensure the completion of remedial action in accordance with paragraph (3).

''(ii) FAILURE TO MEET DEADLINES.—If the Agency Head fails to meet the deadline described in clause (i)(II), additional funds may not be obligated to support expenditures associated with the project until the requirements of this subsection have been fulfilled.

''(f) ADDITIONAL REQUIREMENTS FOR CORE IT INVESTMENT PROJECT REPORTS.—

''(1) INITIAL REPORT.—If a remedial action plan described in subsection (e)(3)(A) has not been submitted for a core IT investment project, the Agency Head, in coordination with the Chief Information Officer and responsible program managers, shall prepare an initial report for inclusion in the first budget submitted to Congress under section 1105(a) of title 31, United States Code, after the designation of a project as a core IT investment project, which includes—

''(A) a description of the primary business case and key functional requirements for the project;

''(B) an identification and description of any portions of the project that have technical requirements of sufficient clarity that such portions may be feasibly procured under firm, fixed-price contracts;

''(C) an independent government cost estimate for the project;

''(D) certification by the Chief Information Officer that all technical and business requirements have been reviewed and validated to ensure alignment with the reported business case; and

''(E) any changes to the primary business case or key functional requirements which have occurred since project inception.

''(2) QUARTERLY REVIEW OF BUSINESS CASE.—The Agency Head, in coordination with the Chief Information Officer and responsible program managers, shall—

''(A) monitor the primary business case and core functionality requirements reported to Congress and the Director for designated core IT investment projects; and

''(B) if changes to the primary business case or key functional requirements for a core IT investment project occur in any fiscal quarter, submit a report to Congress and the Director not later than 14 days after the end of such quarter that details the changes and describes the impact the changes will have on the cost and ultimate effectiveness of the project.

''(3) ALTERNATIVE SIGNIFICANT DEVIATION DETERMINATION.—If the Chief Information Officer determines, subsequent to a change in the primary business case or key functional requirements, that without such change the project would have significantly deviated—

''(A) the Chief Information Officer shall notify the Agency Head of the significant deviation; and

''(B) the Agency Head shall fulfill the requirements under subsection (d)(2) in accordance with the deadlines under subsection (d)(3).

''(4) ALTERNATIVE GROSS DEVIATION DETERMINATION.—If the Chief Information Officer determines, subsequent to a change in the primary business case or key functional requirements, that without such change the project would have grossly deviated—

''(A) the Chief Information Officer shall notify the Agency Head of the gross deviation; and

''(B) the Agency Head shall fulfill the requirements under subsections (e)(2) and (e)(3) in accordance with subsection (e)(4).''.

(b) INCLUSION IN THE BUDGET SUBMITTED TO CONGRESS.—Section 1105(a) of title 31, United States Code, is amended—

(1) in the matter preceding paragraph (1), by striking ''include in each budget the following:'' and inserting ''include in each budget—'';

(2) by redesignating the second paragraph (33) (as added by section 889(a) of Public Law 107–296) as paragraph (35);

(3) in each of paragraphs (1) through (34), by striking the period at the end and inserting a semicolon;

(4) in paragraph (35), as redesignated by paragraph (2), by striking the period at the end and inserting ''; and''; and

(5) by adding at the end the following:

''(36) the reports prepared under section 11317(f) of title 40, United States Code, relating to the core IT investment projects of the agency.''.

(c) IMPROVEMENT OF INFORMATION TECHNOLOGY ACQUISITION AND DEVELOPMENT.—Subchapter II of chapter 113 of title 40, United States Code, is amended by adding at the end the following:

''SEC. 11319. ACQUISITION AND DEVELOPMENT.

''(a) PURPOSE.—The objective of this section is to significantly reduce—

''(1) cost overruns and schedule slippage from the estimates established at the time the program is initially approved;

''(2) the number of requirements and business objectives at the time the program is approved that are not met by the delivered products; and

''(3) the number of critical defects and serious defects in delivered information technology.

''(b) OMB GUIDANCE.—The Director of the Office of Management and Budget shall—

''(1) not later than 180 days after the date of the enactment of this section, prescribe uniformly applicable guidance for agencies to implement the requirements of this section, which shall not include any exemptions to such requirements not specifically authorized under this section; and

''(2) take any actions that are necessary to ensure that Federal agencies are in compliance with the guidance prescribed pursuant to paragraph (1) not later than 1 year after the date of the enactment of this section.

''(c) ESTABLISHMENT OF PROGRAM.—Not later than 120 days after the date of the enactment of this section, each Chief Information Officer, upon the approval of the Agency Head (as defined in section 11317(a) of title 40, United States Code) shall establish a program to improve the information technology (referred to in this section as 'IT') processes overseen by the Chief Information Officer.

''(d) PROGRAM REQUIREMENTS.—Each program established pursuant to this section shall include—

''(1) a documented process for IT acquisition planning, requirements development and management, project management and oversight, earned-value management, and risk management;

''(2) the development of appropriate metrics that can be implemented and monitored on a real-time dashboard for performance measurement of—

''(A) processes and development status of investments;

''(B) continuous process improvement of the program; and

''(C) achievement of program and investment outcomes;

''(3) a process to ensure that key program personnel have an appropriate level of experience, training, and education, at an institution or institutions approved by the Director, in the planning, acquisition, execution, management, and oversight of IT;

''(4) a process to ensure that the agency implements and adheres to established processes and requirements relating to the planning, acquisition, execution, management, and oversight of IT programs and developments; and

''(5) a process for the Chief Information Officer to intervene or stop the funding of an IT investment if it is at risk of not achieving major project milestones.

''(e) ANNUAL REPORT TO OMB.—Not later than the last day of February of each year, the Agency Head shall submit a report to the Office of Management and Budget that includes—

''(1) a detailed summary of the accomplishments of the program established by the Agency Head pursuant to this section;

''(2) the status of completeness of implementation of each of the program requirements, and the date each such requirement was deemed to be completed;

''(3) the percentage of Federal IT projects covered under the program compared to all of the IT projects of the agency, listed by number of programs and by annual dollars expended;

''(4) a detailed breakdown of the sources and uses of the amounts spent by the agency during the previous fiscal year to support the activities of the program;

''(5) a copy of any guidance issued under the program and a statement regarding whether each such guidance is mandatory;

''(6) the identification of the metrics developed in accordance with subsection (b)(2);

''(7) a description of how paragraphs (3) and (4) of subsection (b) have been implemented and any related agency guidance; and

''(8) a description of how agencies will continue to review and update the implementation and objectives of such guidance.

''(f) ANNUAL REPORT TO CONGRESS.—The Director of the Office of Management and Budget shall provide an annual report to Congress on the status and implementation of the program established pursuant to this section.''.

(d) CLERICAL AMENDMENTS.—The table of sections for chapter 113 of title 40, United States Code, is amended—

(1) by striking the item relating to section 11317 and inserting the following:

''11317. Significant and gross deviations.'';

and

(2) by inserting after the item relating to section 11318 the following:

''11319. Acquisition and development.''.

SEC. 5. IT TIGER TEAM.

(a) PURPOSE.—The Director of the Office of Management of Budget (referred to in this section as the ''Director''), in consultation with the Administrator of the Office of Electronic Government and Information and Technology at the Office of Management and Budget (referred to in this section as the ''E-Gov Administrator''), shall assist agencies in avoiding significant and gross deviations in the cost, schedule, and performance of IT investment projects (as such terms are defined in section 11317(a) of title 40, United States Code).

(b) IT TIGER TEAM.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the E-Gov Administrator shall establish a small group of individuals (referred to in this section as the ''IT Tiger Team'') to carry out the purpose described in subsection (a).

(2) QUALIFICATIONS.—Individuals selected for the IT Tiger Team—

(A) shall be certified at the Senior/Expert level according to the Federal Acquisition Certification for Program and Project Managers (FAC–P/PM);

(B) shall have comparable education, certification, training, and experience to successfully manage high-risk IT investment projects; or

(C) shall have expertise in the successful management or oversight of planning, architecture, process, integration, or other technical and management aspects using proven process best practices on high-risk IT investment projects.

(3) NUMBER.—The Director, in consultation with the E-Gov Administrator, shall determine the number of individuals who will be selected for the IT Tiger Team.

(c) OUTSIDE CONSULTANTS.—

(1) IDENTIFICATION.—The E-Gov Administrator shall identify consultants in the private sector who have expert knowledge in IT program management and program management review teams. Not more than 20 percent of such consultants may be formally associated with any 1 of the following types of entities:

(A) Commercial firms.

(B) Nonprofit entities.

(C) Federally funded research and development centers.

(2) USE OF CONSULTANTS.—

(A) IN GENERAL.—Consultants identified under paragraph (1) may be used to assist the IT Tiger Team in assessing and improving IT investment projects.

(B) LIMITATION.—Consultants with a formally established relationship with an organization may not participate in any assessment involving an IT investment project for which such organization is under contract to provide technical support.

(C) EXCEPTION.—The limitation described in subparagraph (B) may not be construed as precluding access to anyone having relevant information helpful to the conduct of the assessment.

(3) CONTRACTS.—The E-Gov Administrator, in conjunction with the Administrator of the General Services Administration (GSA), may establish competitively bid contracts with 1 or more qualified consultants, independent of any GSA schedule.

(d) INITIAL RESPONSE TO ANTICIPATED SIGNIFICANT OR GROSS DEVIATION.—If the E-Gov Administrator determines there is reasonable cause to believe that a major IT investment project is likely to significantly or grossly deviate (as defined in section 11317(a) of title 40, United States Code), including the receipt of inconsistent or missing data, or if the E–Gov Administrator determines that the assignment of 1 or more members of the IT Tiger Team could meaningfully reduce the possibility of significant or gross deviation, the E-Gov Administrator shall carry out the following activities:

(1) Recommend the assignment of 1 or more members of the IT Tiger Team to assess the project in accordance with the scope and time period described in section 11317(c)(1) of title 40, United States Code, beginning not later than 14 days after such recommendation. No member of the Tiger Team who is associated with the department or agency whose IT investment project is the subject of the assessment may be assigned to participate in this assessment. Such limitation may not be construed as precluding access to anyone having relevant information helpful to the conduct of the assessment.

(2) If the E-Gov Administrator determines that 1 or more qualified consultants are needed to support the efforts of the IT Tiger Team under paragraph (1), negotiate a contract with the consultant to provide such support during the period in which the IT Tiger Team is conducting the assessment described in paragraph (1).

(3) Ensure that the costs of an assessment under paragraph (1) and the support services of 1 or more consultants under paragraph (2) are paid by the major IT investment project being assessed.

(4) Monitor the progress made by the IT Tiger Team in assessing the project.

(e) REDUCTION OF SIGNIFICANT OR GROSS DEVIATION.—If the E-Gov Administrator determines that the assessment conducted under subsection (d) confirms that a major IT investment project is likely to significantly or grossly deviate, the E-Gov Administrator shall recommend that the Agency Head (as defined in section 11317(a)(1) of title 40, United States Code) take steps to reduce the deviation, which may include—

(1) providing training, education, or mentoring to improve the qualifications of the program manager;

(2) replacing the program manager or other staff;

(3) supplementing the program management team with Federal Government employees or independent contractors;

(4) terminating the project; or

(5) hiring an independent contractor to report directly to senior management and the E-Gov Administrator.

(f) REPROGRAMMING OF FUNDS.—

(1) AUTHORIZATION.—The Director may direct an Agency Head to reprogram amounts which have been appropriated for such agency to pay for an assessment under subsection (d).

(2) NOTIFICATION.—An Agency Head who reprograms appropriations under paragraph (1) shall notify the Committee on Appropriations of the Senate and the Committee on Appropriations of the House of Representatives of any such reprogramming.

(g) REPORT TO CONGRESS.—The Director shall include in the annual Report to Congress on the Benefits of E-Government Initiatives a detailed summary of the composition and activities of the IT Tiger Team, including—

(1) the number and qualifications of individuals on the IT Tiger Team;

(2) a description of the IT investment projects that the IT Tiger Team has worked during the previous fiscal year;

(3) the major issues that necessitated the involvement of the IT Tiger Team to assist agencies with assessing and managing IT investment projects and whether such issues were satisfactorily resolved;

(4) if the issues referred to in paragraph (3) were not satisfactorily resolved, the issues still needed to be resolved and the Agency Head's plan for resolving such issues;

(5) a detailed breakdown of the sources and uses of the amounts spent by the Office of Management and Budget and other Federal agencies during the previous fiscal year to support the activities of the IT Tiger Team; and

(6) a determination of whether the IT Tiger Team has been effective in—

(A) preventing projects from deviating from the original baseline; and

(B) assisting agencies in conducting appropriate analysis and planning before a project is funded.

SEC. 6. AWARDS FOR PERSONNEL FOR EXCELLENCE IN THE ACQUISITION OF INFORMATION SYSTEMS AND INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Not later than 180 days after the enactment of this Act, the Director of the Office of Personnel Management shall develop policy and guidance for agencies to develop a program to recognize excellent performance by Federal Government employees and teams of such employees in the acquisition of information systems and information technology for the agency.

(b) ELEMENTS.—The program referred to in subsection (a) shall, to the extent practicable—

(1) obtain objective outcome measures; and

(2) include procedures for—

(A) the nomination of Federal Government employees and teams of such employees for eligibility for recognition under the program; and

(B) the evaluation of nominations for recognition under the program by 1 or more agency panels of individuals from government, academia, and the private sector who have such expertise, and are appointed in such a manner, as the Director of the Office of Personal Management shall establish for purposes of the program.

(c) AWARD OF CASH BONUSES.—As part of the program referred to in subsection (a), the Director of the Office of Personnel Management, in consultation with the Director of the Office of Management and Budget, shall establish policies and guidance for agencies to award to any Federal Government employee or teams of such employees recognized pursuant to the program a cash bonus authorized by any other provision of law to the extent that the performance of such individual so recognized warrants the award of such bonus under such provision of law.

Ms. COLLINS. Mr. President. I am pleased to join Senator CARPER in reintroducing a bill that will improve agency performance and Congressional oversight of major federal information-technology, IT, projects. We introduced this bill last Congress and offer it for consideration again because it will strengthen oversight of technology investments to help prevent the waste and misuse of taxpayer dollars.

The well-publicized cost and performance problems with the Census Bureau's handheld computers for the 2010 Census—with its troubling implications for the next House reapportionment and for the allocation of Federal funds—represent only the most recent and conspicuous failure in a long trail of troubles that also includes critical IT projects like the FBI's Virtual Case File initiative.

The 2010 Census is notable among projects that have drawn our attention, not only because of its great scope and expense, but because of its history of unheeded cautions. For years, warnings of potential dangers came from experts sought out by the Census Bureau itself and from the Commerce Department's own Inspector General.

The implications of this lack of proper planning and oversight are evident in the burgeoning estimate for the life-cycle cost of the 2010 Census. The Bureau initially estimated that the 2010 Census would cost the taxpayers about $11.3 billion dollars; today, the estimated cost is more than $14 billion.

Another example is the Department of Homeland Security's, DHS, efforts since 2004 to integrate its financial management systems. DHS spent approximately $52 million on one failed attempt before abandoning the project nearly two years later. According to GAO, this attempt likely failed because DHS had not developed an overall financial management transformation strategy that included financial management policies and procedures, standard business processes, a human capital strategy, and effective internal controls. DHS spent approximately $52 million and now has little, if anything, to show for it.

The Department of Homeland Security is now attempting another consolidation of its financial information technology systems. It is essential that, this time, the Department sufficiently plan and monitor its cost, schedule, and performance targets.

During the 108th Congress, the Committee on Governmental Affairs investigated the botched automated record-keeping project for the federal employees' Thrift Savings Plan, TSP. This project was terminated in 2001 after a four-year contract produced $36 million in waste that was charged to the accounts of TSP participants and beneficiaries. A second vendor needed an additional $33 million to bring the system online, years overdue and costing more than double its original estimate.

In a 2004 letter from the Federal Retirement Thrift Investment Board to the Governmental Affairs Committee, the Board characterized the project as ''ill-fated,'' and acknowledged the importance of careful planning, task definition, communication, proper personnel, and risk management—all of which were lacking on that project.

Large IT project failures have cost US taxpayers literally billions of dollars in wasted expenditures. Perhaps even more troubling is the fact that when Federal IT projects fail, they can undermine the government's ability to defend the nation, enforce its laws, or deliver critical services to citizens. Again and again, we have seen IT project failures grounded in poor planning, ill-defined and shifting requirements, undisclosed difficulties, poor risk management, and lax monitoring of performance.

Unfortunately, as the Government Accountability Office, GAO, continues to report, Federal IT projects still fall short in their use of effective oversight techniques to monitor development and to spot signs of possible trouble.

The GAO reported that the Federal Government spent over $71 billion in fiscal year 2009 on IT projects. Most of that spending was concentrated in two dozen agencies that have approximately 800 major projects underway.

When the GAO reviewed a random sampling of these major Federal IT projects, they found that 85—nearly half the sample—had been ''rebaselined.'' Eighteen of those projects have been rebaselined three or more times. For example, the Department of Defense Advanced Field Artillery Tactical Data System has been rebaselined four times; a Veterans Affairs Health Administration Center project has been rebaselined 6 times.

Rebaselining can reflect funding changes, revisions in project scope or goals, and other perfectly reasonable project modifications. But as the GAO notes, ''[rebaselining] can also be used to mask cost overruns and schedule delays.'' All major federal agencies have rebaselining policies, but the GAO concludes that they are not comprehensive and that ''none of the policies are fully consistent with best practices.''

The bill that Senator CARPER and I are introducing will go far toward addressing the weaknesses identified by the GAO and will reduce the risks that important Federal IT projects will drag on far beyond deadlines, fail to deliver intended capabilities, or waste taxpayers' money.

Our bill will improve both agency and Congressional oversight of large Federal IT projects. For all major investments, the bill requires agencies to track the Earned Value Management index, a key cost and performance measure, and to alert Congress should that measure fall below a defined threshold.

The bill requires additional reports to Congress as well as specific corrective actions should those same indicators continue to worsen. Further, because the bill's performance thresholds are based on original cost baselines, rebaselining can no longer serve as a tactic to hide troubled projects. Where severe shortfalls remain uncorrected, agencies are prohibited from committing additional funds to the project until the required corrective actions are taken.

Our bill would not make Congress a micro-manager of Federal projects—especially in so complex a field as information technology. But it will ensure that, for these important investments, agencies will be required to track key performance metrics, inform Congress of shortfalls in those metrics, and provide Congress with follow-up reports, independent cost estimates, and analyses of project alternatives when the original projects have run off course.

The bill also provides that each covered agency identify to Congress their top mission-critical projects. Those ''core investments'' would be subject to additional upfront planning, reporting, and performance monitoring requirements. This will help ensure that agencies apply extra vigilance to these projects at the planning stage, and not just when execution begins.

In addition to tracking cost and schedule slippage, agencies making

core IT investments must provide a complete ''business case'' that outlines the need for the project and its associated costs and schedules; produce a rigorous, independent, third-party estimate of the project's full, life-cycle costs; have the agency CIO certify the project's functional requirements; track these functional requirements; and report to Congress any changes in functional requirements, including whether those changes concealed a major cost increase.

To help agencies deliver IT projects on time and on budget, the bill also provides two new support mechanisms.

First, agency heads would be required to establish an internal IT-management program, subject to OMB guidelines, to improve project planning, requirements development, and management of earned value and risk.

Second, the Director of OMB and its E-Gov Administrator would be required to establish an IT Tiger Team of experts and independent consultants that can be assigned to help agencies reform troubled projects. In addition, the E-Gov Administrator can recommend that agency heads mentor or replace an IT project manager, reinforce the management team, terminate the project, or hire an independent contractor to report on the project.

These and other provisions will help improve project planning, avoid problems in project execution, provide early alerts when problems arise, and promote prompt corrective action.

In projects where difficulties persist, our bill provides strong remedies. For projects that exhibit a performance shortfall of 20 percent or more, the agency head involved must not only alert Congress but also provide a summary of a concrete plan of action to correct the problem. If the shortfall exceeds 40 percent, agencies have six months to take required remedial steps or else suspend further project spending until those steps are completed.

If the provisions of this bill had been in force during the past decade, early indicators of trouble and prompt warnings to Congress might have helped prevent much of the added cost, decreased functionality, and increased anxiety we now see surrounding the handheld computers that were intended to streamline the 2010 Census. The additional scrutiny of plans and costs required by this bill might have saved some of the billions wasted on other IT projects that ultimately landed on high-risk lists.

I urge every Senator to support this much-needed and bipartisan bill.

By Mr. CARPER:

S. 921. A bill to amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

Mr. CARPER. 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 placed in the RECORD, as follows:

S. 921

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 ''United States Information and Communications Enhancement Act of 2009'' or the ''U.S. ICE Act of 2009''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) The development of an interconnected global information infrastructure has significantly enhanced the productivity, prosperity, and collaboration of people, business, and governments worldwide.

(2) The information infrastructure of the United States is a strategic national resource vital to our democracy, economy, and security.

(3) The Federal Government must increasingly rely on a trusted and resilient information infrastructure to effectively and efficiently communicate with and deliver services to citizens, enhance economic prosperity, defend the Nation from attack, and recover from natural disasters.

(4) Since 2002 the Federal Government has experienced multiple high-profile breaches that resulted in the theft of sensitive information amounting to more than the entire print collection contained in the Library of Congress, including personally identifiable information, advanced scientific research, and prenegotiated United States diplomatic positions.

(5) On March 12, 2008 witnesses testified before a hearing held by the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security of the Committee on Homeland Security and Governmental Affairs of the Senate that—

(A) implementation of the Federal Information Security Management Act of 2002 (Public Law 107–296; 116 Stat. 2135) wastes agency resources on paperwork exercise instead of security;

(B) agencies do not fully understand what information they hold, who has access to that information, and whether the information has been compromised; and

(C) agencies lack effective coordination for mitigating and responding to cyber-related incidents.

(6) The Federal Information Security Management Act of 2002 (Public Law 107–296; 116 Stat. 2135) needs to be amended to increase the coordination of agency activities to enhance situational awareness throughout the Federal Government using more effective enterprise-wide automated monitoring, detection, and response capabilities.

SEC. 3. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Definitions

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

''(b) In this subchapter:

''(1) The term 'adequate security' means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification, of information.

''(2) The term 'Director' means the Director of the National Office for Cyberspace.

''(3) The term 'incident' means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

''(4) The term 'information infrastructure' means the underlying framework that information systems and assets rely on in processing, transmitting, receiving, or storing information electronically.

''(5) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, which means ensuring timely and reliable access to and use of information.

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

''(7)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''§ 3552. National Office for Cyberspace

''(a) There is established within the Executive Office of the President an office to be known as the National Office for Cyberspace.

''(b) There shall be at the head of the Office a Director who shall be appointed by the President, by and with the advice and consent of the Senate. The Director of the National Office for Cyberspace shall administer all functions under this subchapter and collaborate to the extent practicable with the heads of the appropriate agencies, the private sector, and international partners. The Office shall serve as the principal office for coordinating issues relating to achieving an assured, reliable, secure, and survivable

global information and communications infrastructure and related capabilities.

"§ 3553. Authority and functions of the National Office for Cyberspace

''(a) The Director shall develop and implement a comprehensive national cyberspace strategy to ensure a trusted and resilient communications and information infrastructures that—

''(1) enhances economic prosperity and facilitates market leadership for the United States information and communications industry;

''(2) deters, prevents, detects, defends against, responds to, and remediates interruptions and damage to United States information and communications infrastructure;

''(3) ensures United States capabilities to operate in cyberspace in support of national goals; and

''(4) protects privacy rights and preserving civil liberties of United States persons.

''(b) Notwithstanding any provision of law, regulation, rule, or policy to the contrary, the National Office for Cyberspace may—

''(1) direct the sponsorship of the security clearances for Federal officers and employees (including experts and consultants employed under section 3109) whose responsibilities involve critical infrastructure in the interest of national security; and

''(2) employ experts and consultants under section 3109 for cyber security-related work.

''(c) With respect to responsibilities with the Federal Government, the National Office for Cyberspace shall—

''(1) provide recommendations to agencies on measures that shall be required to be implemented to mitigate vulnerabilities, attacks, and exploitations discovered as a result of activities required pursuant to this section;

''(2) oversee the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 3556;

''(3) to the extent practicable—

''(A) prioritize the policies, principles, standards, and guidelines developed under section 3556 based upon the threat, vulnerability and consequences of an information security incident; and

''(B) develop guidance that requires agencies to actively monitor the effective implementation of policies, principles, standards, and guidelines developed under section 3556;

''(4) require agencies, consistent with the standards promulgated under such section 3556 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(A) information collected or maintained by or on behalf of an agency; or

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

''(5) coordinate and ensure that the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and standards and guidelines developed for national security systems are, to the maximum extent practicable, complementary and unified;

''(6) oversee agency compliance with the requirements of this subchapter, including coordinating with the Office of Management and Budget to use any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

''(7) review at least annually, and approving or disapproving, agency information security programs required under section 3554(b); and

''(8) coordinate information security policies and procedures with related information resources management policies and procedures.

''(d)(1) After consultation with the appropriate agencies, the Director shall oversee the effective implementation of government-wide operational evaluations on a frequent and recurring basis to evaluate whether agencies effectively—

''(A) monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations;

''(B) report to and collaborate with the appropriate public and private security operation centers and law enforcement agencies; and

''(C) mitigate the risk posed by previous successful exploitations in a timely fashion and in order to prevent future vulnerabilities, attacks, and exploitations.

''(2) Not later than 30 days after receiving an operational evaluation under this subsection, the Director shall ensure agencies evaluated under paragraph (1) develop a plan for addressing recommendations and mitigating vulnerabilities contained in the security reports identified under paragraph (1), including a timeline and budget for implementing such plan.

''(e) Not later than March 1 of each year, the Director shall submit a report to Congress on the overall information security posture of the communications and information infrastructure of the United States, including—

''(1) the evaluations conducted under subsection (d) for the United States Government;

''(2) a detailed assessment of the overall resiliency of the communications and information infrastructure effectiveness of the United States and the United States Government including the ability to monitor, detect, mitigate, and respond to an incident;

''(3) a detailed assessment the information security effectiveness of each agency, including the ability to monitor, detect, mitigate, collaborate, and respond to an incident;

''(4) a detailed assessment of operational evaluations performed during the preceding fiscal year, the results of such evaluations, and any actions that remain to be taken under plans included in corrective action reports under subsection (d);

''(5) a detailed assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 3554, and recommendations for enhancement;

''(6) a detailed assessment of significant deficiencies in the information security and reporting practices of the Federal Government as applicable to each agency;

''(7) planned remedial action to address deficiencies described under paragraph (6), including an associated budget and recommendations for relevant executive and legislative branch actions;

''(8) a summary of the results of the independent evaluations under section 3555; and

''(9) a detailed assessment of the effectiveness of reporting to the National Cyber Investigative Joint Task Force under section 3554.

''(f) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

''(g)(1) In collaboration with the private sector and in coordination with the Director of the Office of Management and Budget, the National Institute of Standards and Technology, and the General Service Administration, the Director shall develop and implement policy, guidance, and regulations that cost effectively enhance the security of the Federal Government, including policy, guidance, and regulations that—

''(A) to the extent practicable, standardize security requirements (also known as 'lockdown configurations') of commercial off-the-shelf products and services (including cloud products and services) purchased by the Federal Government;

''(B) to the extent practicable, obtain products and services with security configuration baselines consistent with available security standards and configurations and guidelines developed by the National Institute of Standards and Technology;

''(C) incentivize agencies to purchase standard products and services through the General Service Administration in order to reduce the vulnerabilities and costs associated with custom products and services; and

''(D) enable purchasing decisions to reasonably and appropriately account for significant supply chain security risks associated with any particular product or service.

''(2) Not later than 180 days after the date of enactment of the United States Information and Communications Enhancement Act of 2009, and annually thereafter, the Director shall submit a report to Congress that includes—

''(A) a description of the cost savings and security enhancements that can be achieved by using the purchasing power of the Federal Government; and

''(B) recommendations for legislative or executive branch actions necessary to achieve such cost savings.

"§ 3554. Agency responsibilities

''(a) The head of each agency shall—

''(1) be responsible for—

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

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

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

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

''(i) information security standards promulgated under section 3556;

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

''(iii) ensuring the standards implemented for information systems and national security systems under the agency head are complementary and uniform, to the extent practicable; and

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

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

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

''(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 3556, for information security classifications and related requirements;

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

''(D) continuously testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

''(3) delegate to an agency official designated as the Chief Information Security Officer the authority to ensure and enforce compliance with the requirements imposed on the agency under this subchapter, including—

''(A) overseeing the establishment and maintenance of a security operations capability that on an automated and continuous basis can—

''(i) detect, report, respond to, contain, and mitigate incidents that impair adequate security of the information and information infrastructure, in accordance with policy provided by the Director, in consultation with the Chief Information Officers Council, and guidance from the National Institute of Standards and Technology;

''(ii) collaborate with the National Office for Cyberspace and appropriate public and private sector security operations centers to address incidents that impact the security of information and information infrastructure that extend beyond the control of the agency; and

''(iii) not later than 24 hours after discovery of any incident described under subparagraph (A), unless otherwise directed by policy of the National Office for Cyberspace, provide notice to the appropriate security operations center, the National Cyber Investigative Joint Task Force, and inspector general;

''(B) collaborating with the Administrator for E–Government and the Chief Information Officer to establish, maintain, and update an enterprise network, system, storage, and security architecture framework documentation to be submitted quarterly to the National Office for Cyberspace and the appropriate security operations center, that includes—

''(i) documentation of how technical, managerial, and operational security controls are implemented throughout the agency's information infrastructure; and

''(ii) documentation of how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

''(I) the policy of the Director;

''(II) the National Institute of Standards and Technology guidance; and

''(III) the Chief Information Officers Council recommended approaches;

''(C) developing, maintaining, and overseeing an agency wide information security program as required by subsection (b);

''(D) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under sections 3553 and 3556;

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

''(F) assisting senior agency officials concerning their responsibilities under paragraph (2);

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

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

''(6) ensure that the Chief Information Security Officer possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and has information security duties as the primary duty of that official.

''(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3553(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

''(1) periodic assessments—

''(A) of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; and

''(B) that recommend a prioritized description of which data and applications should be removed or migrated to more secure networks or standards;

''(2) penetration tests commensurate with risk (as defined by the National Institute of Standards and Technology and the National Office for Cyberspace) for agency information systems; and

''(3) information security vulnerabilities are mitigated based on the risk posed to the agency;

''(4) policies and procedures that—

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

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

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

''(D) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 3556;

''(iii) minimally acceptable system configuration requirements, as determined by the Director; and

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

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

''(6) role-based security awareness training to inform personnel with access to the agency network, including contractors and other users of information systems that support the operations and assets of the agency, of—

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

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

''(7) to the extent practicable, automated and continuous technical monitoring for testing, and evaluation of the effectiveness and compliance of information security policies, procedures, and practices, including—

''(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(b); and

''(B) management, operational, and technical controls relied on for an evaluation under section 3555;

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

''(9) to the extent practicable, continuous technical monitoring for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued by the Director, including—

''(A) mitigating risks associated with such incidents before substantial damage is done;

''(B) notifying and consulting with the appropriate security operations response center; and

''(C) notifying and consulting with, as appropriate—

''(i) law enforcement agencies and relevant Offices of Inspectors General;

''(ii) the National Office for Cyberspace; and

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

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

''(c) Each agency shall—

''(1) submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b) to—

''(A) the National Office for Cyberspace;

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

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

''(D) the Committee on Government Oversight and Reform of the House of Representatives;

''(E) the Committee on Homeland Security of the House of Representatives;

''(F) other appropriate authorization and appropriations committees of Congress; and

''(G) the Comptroller General.

''(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

''(A) annual agency budgets;

''(B) information resources management of this subchapter;

''(C) information technology management under this chapter;

''(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

''(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

''(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note);

''(G) internal accounting and administrative controls under section 3512 of title 31; and

''(H) performance ratings, salaries, and bonuses provided to the Chief Information Security Officer and supporting personnel taking into account program performance; and

''(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

''(A) as a material weakness in reporting under section 3512 of title 31; and

''(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial

Management Improvement Act (31 U.S.C. 3512 note).

''(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the National Office for Cyberspace, shall include as part of the performance plan required under section 1115 of title 31 a description of—

''(A) the time periods; and

''(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

''(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1) and operational evaluations required under section 3553(d).

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

''§ 3555. Annual independent evaluation

''(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

''(2) Each evaluation under this section shall consist of—

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

''(B) an assessment (made on the basis of the results of the testing) of compliance with—

''(i) the requirements of this subchapter; and

''(ii) related information security policies, procedures, standards, and guidelines.

''(b)(1) For each agency with an Inspector General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.

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

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

''(d) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

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

''(f) The Comptroller General shall—

''(1) not later than 180 days after the date of enactment of the United States Communications and Information Enhancement Act of 2009 and after collaboration with the Director and the Inspectors General, develop and deliver standards for independent evaluations as required under this section that are risk-based and cost effective;

''(2) periodically evaluate and report to Congress on—

''(A) the adequacy and effectiveness of agency information security policies and practices; and

''(B) the implementation of the requirements of this subchapter.

''§ 3556. Responsibilities for Federal information systems standards

''(a)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), prescribe standards and guidelines pertaining to information systems, including national security systems.

''(2)(A) Standards prescribed under subsection (a)(1) shall include information security standards that—

''(i) to the extent practicable, are unified with standards and guidelines developed for information systems and national security systems to ensure the adequacy and effectiveness of information security and information sharing;

''(ii) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(iii) are otherwise necessary to improve the security of information and information systems, including information stored by third parties on behalf of the Federal Government.

''(B) Information security standards described in subparagraph (A) shall be compulsory and binding.

''(b) The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

''(c) To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget and the National Office for Cyberspace.

''(d) The National Office for Cyberspace and the head of an agency may employ standards for the cost effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards—

''(1) contain at least the applicable standards made compulsory and binding by the Secretary; and

''(2) are otherwise consistent with policies and guidelines issued under section 3553.

''(e) The decision by the Secretary regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).''.

SEC. 4. AUTHORITY AND RESPONSIBILITY OF THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM IN RELATION TO FEDERAL AGENCIES.

(a) DEFINITION.—In this section:

(1) The term ''agency'' has the meaning given under section 3502(1) of title 44, United States Code.

(2) The term ''US–CERT'' means the United States Computer Emergency Readiness Team.

(b) PURPOSES.—The purposes of this section are to recognize that US–CERT—

(1) is charged with providing response support and defense against cyber attacks for agencies and information sharing and collaboration with State and local government, industry, and international partners;

(2) interacts with agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cyber security information to the public;

(3) provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States Government about cyber security; and

(4) has continually enhanced its ability to monitor, detect, and respond to information security incidents that affect the Federal Government.

(c) COORDINATION WITH US–CERT.—The head of each agency shall ensure that the Chief Information Officer, Chief Information Security Officer, and security operations centers under the direction of that agency head shall establish policies, procedures, and guidance to effectively coordinate with the Director of US–CERT in a timely fashion to detect, report, respond to, contain, and mitigate incidents that impair adequate security of the information and information infrastructure.

(d) REVIEW AND APPROVAL.—In coordination with the Administrator for Electronic Government and Information Technology, the Director of the National Office for Cyberspace shall review and approve the policies, procedures, and guidance established in subparagraph (c) to ensure that US–CERT has the capability to effectively and efficiently detect, correlate, respond to, contain, and mitigate incidents that impair the adequate security of the information and information infrastructure of more than 1 agency. To the extent practicable, the capability shall be continuous and technically automated.

(e) SECURITY CLEARANCES; EXPERTS AND CONSULTANTS.—Notwithstanding any provision of law, regulation, rule, or policy to the contrary, the Director of US-CERT may—

(1) direct the sponsorship of the security clearances for Federal officers and employees (including experts and consultants employed under section 3109) whose responsibilities involve critical infrastructure in the interest of national security; and

(2) employ experts and consultants under section 3109 for cyber security-related work.

SEC. 5. AUTHORITY AND RESPONSIBILITY OF DEPARTMENTS NOT RELATED TO MILITARY FUNCTIONS.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency''—

(A) means—

(i) an Executive department defined under section 101 of title 5, United States Code; and

(ii) an Executive agency that has multiple components which have separate and distinct enterprise architectures; and

(B) shall not include—

(i) the Department of Defense; or

(ii) any component of an Executive agency that is performing any national security function, including military intelligence.

(2) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given under section 105 of title 5, United States Code.

(b) PURPOSE.—The purpose of this section is to recognize that—

(1) agencies have developed and maintained separate and distinct enterprise architectures that inhibit the ability of an agency to ensure that components of that agency have effectively implemented security policies, procedures, and practices;

(2) the separate and distinct enterprise architectures have in many instances been at

the detriment of securing the agency information infrastructure (the civilian cyberspace) and exposed that infrastructure to unnecessary risk for an extended period of time; and

(3) a more uniform agency enterprise architecture will be more efficient and effective for the purposes of information sharing and ensuring the appropriate confidentiality, integrity, and availability of information and information systems.

(c) AGENCY COORDINATION.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall ensure that components of that agency shall establish an automated reporting mechanism that allows the Chief Information Security Officer and security operations center at the total agency level to implement and monitor the implementation of appropriate security policies, procedures, and controls of agency components.

(2) APPROVAL AND COORDINATION.—The activities conducted under paragraph (1) shall be—

(A) approved by the Director of the National Office for Cyberspace; and

(B) to the extent practicable, in coordination and complementary with activities—

(i) described under section 4; and

(ii) conducted by the Administrator for E-Government and Information Technology.

SEC. 6. TECHNICAL AND CONFORMING AMENDMENTS.

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

''SUBCHAPTER II—INFORMATION SECURITY

''Sec. 3551. Definitions.

''Sec. 3552. National Office for Cyberspace.

''Sec. 3553. Authority and functions of the National Office for Cyberspace.

''Sec. 3554. Agency responsibilities.

''Sec. 3555. Annual independent evaluation.

''Sec. 3556. Responsibilities for Federal information systems standards.''.

(b) OTHER REFERENCES.—

(1) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3551(b)''.

(2) Section 2222(j)(6) of title 10, United States Code, is amended by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(3) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(4) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(5) Section 20(a)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by striking ''section 3532(b)(2)'' and inserting ''section 3551(b)''.

(6) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)''.

SEC. 7. EFFECTIVE DATE.

This Act (including the amendments made by this Act) shall take effect 30 days after the date of enactment of this Act.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 115—RECOGNIZING THE CRUCIAL ROLE OF ASSISTANCE DOGS IN HELPING WOUNDED VETERANS LIVE MORE INDEPENDENT LIVES, EXPRESSING GRATITUDE TO THE TOWER OF HOPE, AND SUPPORTING THE GOALS AND IDEALS OF CREATING A TOWER OF HOPE DAY

Mr. LIEBERMAN submitted the following resolution; which was referred to the Committee on Veterans' Affairs:

S. RES. 115

Whereas the brave men and women defending America's democracy in Iraq and Afghanistan are in harm's way;

Whereas thousands of America's returning veterans were seriously wounded in combat, including brain injuries, single and double amputations, and other traumatic wounds;

Whereas these brave soldiers return to the United States and spend weeks, months, and years in hospitals recovering, and return to their homes needing assistance to regain their independence;

Whereas these recovering soldiers who are teamed up with assistance dogs lead more comfortable and more independent lives;

Whereas these dogs provide assistance to wounded veterans while walking, going up and down stairs, and getting up from a sitting or fallen position, and also pick up dropped articles, retrieve items from a distance, pull manual wheelchairs a short distance, turn lights on and off, and perform other important daily tasks;

Whereas assistance animals offer priceless companionship and unconditional love on a daily basis;

Whereas there are fewer than 75 veterans from Iraq and Afghanistan who currently have assistance dogs, as many veterans cannot afford them or do not know about the benefits that assistance dogs provide;

Whereas severely wounded veterans currently have to wait up to 2 years before they can receive an assistance animal;

Whereas The Tower of Hope was created following the attacks of September 11, 2001, to bring hope to wounded veterans by providing them with assistance dogs at no cost; and

Whereas The Tower of Hope has substantially improved many lives by raising funds for the training of assistance dogs, providing grants for American combat wounded veterans, and advocating for the benefits of these animals: Now, therefore, be it

Resolved, That the Senate—

(1) acknowledges the importance of assistance dogs in helping combat-wounded veterans live happier and more independent lives;

(2) applauds the outstanding work of The Tower of Hope and its dedication to training and providing assistance dogs to wounded veterans, as well as educating people about the benefits of such animals;

(3) expresses deep gratitude and support to volunteers and donors who have made this great program possible by generously offering time and funds;

(4) encourages the general public to support wounded veterans by volunteering or donating to help train assistance dogs;

(5) calls for a vigorous promotion of, and advocacy for, the benefits of assistance animals to physicians and the general public; and

(6) supports the goals and ideals of creating a Tower of Hope Day in honor of wounded American veterans and their service dogs, the work of The Tower of Hope, and the many generous donors.

SENATE RESOLUTION 116—COMMENDING THE HEAD COACH OF THE UNIVERSITY OF KANSAS MEN'S BASKETBALL TEAM, BILL SELF, FOR WINNING THE HENRY P. IBA COACH OF THE YEAR AWARD PRESENTED BY THE UNITED STATES BASKETBALL WRITERS ASSOCIATION AND FOR BEING NAMED THE SPORTING NEWS NATIONAL COACH OF THE YEAR AND THE BIG 12 COACH OF THE YEAR

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

S. RES. 116

Whereas after the University of Kansas men's basketball team won the 2008 National Collegiate Athletic Association (NCAA) Men's Basketball Division I Championship, all the most experienced players on the team went on to graduate or pursue their professional ambitions;

Whereas, despite this challenge, the Head Coach of the University of Kansas men's basketball team, Bill Self, led the 2009 team to an impressive 27–win season, in which the team ended the regular season at the top of the Big 12 Conference, and finished the 2009 NCAA Men's Basketball Division I tournament in the Sweet Sixteen;

Whereas, Coach Self has been a head coach for 16 years, winning 9 league championships in the last 11 years and guiding his teams through 11 consecutive 20-win seasons;

Whereas Coach Self is 1 of only 4 coaches in NCAA Men's Basketball Division I history to have led 3 different schools (the University of Tulsa, the University of Illinois, and the University of Kansas) to the Elite Eight in the NCAA Men's Basketball Division I tournament;

Whereas Coach Self has demonstrated the Kansas values of hard work, determination, pride, and spirit, and has instilled these values in the athletes he coaches;

Whereas during his career at the University of Kansas, Coach Self has coached 11 professional basketball players, and impacted the lives of hundreds of young men;

Whereas in 2009, Coach Self won the Henry P. Iba Coach of the Year Award presented by the United States Basketball Writers Association and was named the Sporting News National Coach of the Year and the Big 12 Coach of the Year; and

Whereas Coach Self is an asset to the country, the State of Kansas, and the University of Kansas: Now, therefore, be it

Resolved, That the Senate—

(1) commends the Head Coach of the University of Kansas men's basketball team, Bill Self, for—

(A) winning the Henry P. Iba Coach of the Year Award presented by the United States Basketball Writers Association; and

(B) being named the Sporting News National Coach of the Year and the Big 12 Coach of the Year; and

(2) respectfully requests the Secretary of the Senate to transmit an enrolled copy of this resolution for appropriate display to—

(A) the Chancellor of the University of Kansas, Robert Hemenway;

(B) the Athletic Director of the University of Kansas, Lew Perkins; and

(C) the Head Coach the University of Kansas men's basketball team, Bill Self.