We see that on this chart. We show a $52 billion surplus, but the fact is, we are truly in deficit because we will be using $122 billion of Social Security in 2002, $125 billion in 2003, and so forth. So we are going to be using the Social Security surplus according to this chart three out of the year 2006.

I remind my colleagues the projected $52 billion unified surplus is a gross exaggeration of the possible surplus this year because we have pledged we are going to use $60 to $75 billion of interest payments and discouraging economic activity.

Remember, low interest rates are important to the economy. In fact, Federal Reserve Chairman Alan Greenspan has been quite clear about this as he has highlighted this in the past few weeks. As my colleagues know, Congress will consider a true stimulus package in the near future. Helping America’s workers, all workers, should be a part of that package and should be our No. 1 priority.

The stimulus package can only be so big. So it is critical that we touch as many Americans as possible. All of them must be included in that economic stimulus package. That same message applies to the money we allocate to fight terrorism at home and abroad. We need to prioritize and we need to get the biggest bang for our buck, literally and figuratively.

We in this body must never lose sight that the day of reckoning with the baby boomer retirement has not just been put off by our current crisis. Like it or not, the baby boomers will begin to retire in about 10 years, and if we fail to act, we will put an unacceptable burden on our children and grandchildren.

We face an important challenge in preparing for that day. Our goal should be to fund our war on terrorism at home and abroad, respond to the needs of the victims of the terrorist attack in New York and elsewhere, and get our economy going, and as soon as possible, end deficit spending. We owe it to our children and grandchildren.

I yield the floor.

Mr. REID. Mr. President, I appreciate the Senator yielding.

Mr. LEAHY. Mr. President, what is the time agreement that we are now operating under?

The PRESIDING OFFICER. There are 4 hours equally divided. In addition, there are 40 minutes on each of the four amendments to be offered by the Senator from Wisconsin, Mr. FEINGOLD.

Mr. LEAHY. I thank the distinguished Presiding Officer.

I cannot help but look back at our distinguished President, the senior Senator from New York, how much his State has suffered. Both he and his distinguished colleague, Senator Clinton, have spoken eloquently, both on the floor and elsewhere, about that. I know in my own private conversations with the distinguished President I felt the depth of his grief and emotion for a city that he obviously and unabashedly loves. His references to New York City over the years are almost similar to the kind of comments I make about Vermont. But I do note the accent is somewhat different. I assume it is because of the Vermont accent.

But I think the Senators from New York, and the Senators from New Jersey and Connecticut have especially spoken of the effect on families and loved ones in the New York area. People who work there are from New York, New Jersey, and Connecticut, I know how sad they feel.

I think of the people who died in Pennsylvania in an airplane that was hijacked planning a trip to the very building we are in—this symbol of democracy. Only with a great loss of life did it not happen. But there would be an enormous disruption in our Government. The next day, the view that most people around the world have—our symbol of democracy—would be gone.

I think of the brave men and women who died, as the President and others have said, doing their duty at the Pentagon, and the hundreds—even thousands—of children who went to school happily in the morning and came home to find that they were orphans.

It was a terrible, horrible day.

I think back to what happened in Oklahoma City in 1995 and the actions we took then. We are moving, of course, much faster now than we did at that time, and I hope perhaps with more people of the Senate.

We have before us the USA Act of 2001. I worked with Chairman SENSENBRINNER and Congressman CONyers...
and Republican and Democratic leaders in the House because I hope Congress can act swiftly to enact this measure. Some may be concerned if we have a conference—because the House is somewhat different than the Senate—that we could not resolve our differences on these issues. That happened after Oklahoma City. That legislation took nearly a year to reconcile.

I believe the American people and my fellow Senators, both Republican and Democratic, deserve faster final action. I assure the Senate, when we go to conference, we will complete that conference very quickly. We have demonstrated the ability in this body—and also Senators who have worked with me on both sides of the aisle and our staff—that we can work around the clock.

The distinguished senior Senator from Utah, Mr. Hatch, and I have been working together in constant communication on this matter.

Last Thursday, October 4, I was pleased to introduce, along with the majority leader, Senator Daschle, and the Republican leader, Senator Lott, also the chairman of the Banking and Intelligence Committees, Senator Sarbanes, Senator Graham of Florida, Senator Hatch, and Senator Shelby, the USA Act.

I must say this bill is not the bill I would have written if I were the only one writing it. I dare say it is not the bill the distinguished President Officer, one of the brightest and most accomplished people I know, would have written, if he were writing it. It is not the bill the distinguished chairman of the Banking Committee would have written if he were writing it. It is not the bill the distinguished ranking member, Mr. Hatch, would have written when he was chairman, if he was solely writing the bill. It is really not the bill that any one of the other Members would have written. We can’t pass 100 bills. We have tried to put together the best possible bill. Of course, Republican and Democratic colleagues must come together, and that is what we did. I should point out that this is not the bill the administration, through the Attorney General, delivered to us and asked for immediate passage. We actually did the administration a favor because rather than take the bill they dropped and said pass immediately, we did something that apparently they had not done. We read it and were able to refine and supplement their proposal in a number of ways. We were able to remove a number of unconstitutional parts. The administration accepted the amendments to the final bill that I proposed to improve our security on the Northern Border to assist our State, Federal, and local law enforcement officers and provide compensation to the victims of terrorist acts and to the public safety officers that gave their lives to protect us.

It also provides proposed checks on Government powers—checks that were not contained in the Attorney General’s initial proposal.

In negotiations with the administration, I have done my best to strike a reasonable balance between the need to address the threat of terrorism, which we all recognize is growing at this time, and the need to protect our constitutional freedoms. Despite my misgivings, I have acquiesced in some of the administration’s proposals because it is important to preserve national unity in this time of national crisis and to move the legislative process forward.

We still have room for improvement. Even after the Senate passes judgment on this bill—I believe it will tonight—the debate is not going to be finished because we have to consider those important things done in the other body. What I have done throughout this time is to remember the words of Benjamin Franklin—when he literally had his neck on the line because if the Revolution had failed, he and the others would have been hanged—when he said: A people who would trade their liberty for security deserve neither.

We protected our security, but I am not going to give up the liberties that Americans have spent 220 years to obtain.

Moreover, our ability to make rapid progress was impeded because the negotiations with the Administration did not always occur in the best possible way. On several key issues that are of particular concern to me, we had reached an agreement with the Administration on Sunday, September 30. Unfortunately, within two days, the Administration announced that it was reneging on the deal. I appreciate the complex task of considering the concerns and missions of multiple federal agencies, and that sometimes agreements must be modified as their implications are scrutinized by affected agencies. When agreements have been made, the Administration must be withdrawn and negotiations on resolved issues reopened, those in the Administration who blame the Congress for delay with what the New York Times described last week as “scurrilous remarks,” do not help the process move forward.

Hearings. We have expedited the legislative process in the Judiciary Committee to consider the Administration’s proposals. In daily news conferences, I have referred to the need for such prompt consideration. I commend him for making the time to appear before the Judiciary Committee at a hearing September 25 to respond to questions from all the Members from both parties have about the Administration’s initial proposals. I also thank the Attorney General for extending the hour and a half he was able to make in his schedule for the hearing for another fifteen minutes so that Senator Feinstein and Senator Specter could ask him questions before his departure. I regret that the Attorney General did not have the time to respond to questions from all the Members of the committee either on September 25 or last week, but again thank him for the attention he promised to give to written questions Members submitted about the legislation. We have not received answers to those written questions in advance, but I make them a part of the hearing whenever they are sent.

The Chairman of the Constitution Subcommittee, Senator Feingold, also held an important hearing on October 3 on the civil liberties ramifications of the expanded surveillance powers requested by the Administration. I thank him for his assistance in illuminating these critical issues for the Senate.

Rule 14. To accommodate the Administration’s request for prompt consideration of this legislation, the Leaders decided to hold the USA Act at the desk rather than refer the bill to the Committee for mark-up, as is regular practice. Senator S. 783 aimed at refining the Victims of Terrorism Act of 1996 (VOTA), and Improving the manner in which the Crime Victims Fund is managed and preserved. Most significantly, section 621

October 11, 2001
of the USA Act will eliminate the cap on VOCA spending, which has prevented more than $700 million in Fund deposits from reaching victims and supporting essential services.

Congress has capped spending from the first two fiscal years, and President Bush has proposed a third cap for fiscal year 2002. These limits on VOCA spending have created a growing sense of confusion and unease by many of those concerned about the future of the Fund. We should not be imposing artificial caps on VOCA spending while substantial unmet needs continue to exist. Section 621 of the USA Act replaces the cap with a self-regulating system that will ensure stability and protection of Fund assets, while allowing more money to be distributed to the States for victim compensation and assistance.

Other provisions included from S. 783 will ensure a more immediate and effective assistance to the victims of terrorism. Shortly after the Oklahoma City bombing, I proposed and the Congress adopted the Victims of Terrorism Act of 1995. This legislation authorized the OVC to set aside a reserve fund of up to $50 million as part of the Crime Victims Fund. The emergency reserve was intended to serve as a "rainy day" fund to supplement compensation and assistance grants to states to provide emergency relief in the wake of an act of terrorism or mass violence that might otherwise overwhelm the resources of a State's crime victim compensation program and crime victim assistance services. Last month's disaster created vast needs that have all but depleted the reserve. Section 621 of the USA Act authorizes OVC to replenish the reserve with up to $50 million, and streamlines the mechanism for replenishment of the Fund.

Another critical provision of the USA Act will enable OVC to provide more immediate and effective assistance to victims of terrorism and mass violence occurring within the United States. I proposed this measure last year as an amendment to the Justice for Victims of Terrorism Act, but was compelled to drop it to achieve bipartisan consensus. I am pleased that we are finally getting it done this year.

The recent changes in VOCA reforms in the USA Act are long overdue. Yet, I regret that we are not doing more. In my view, we should pass the Crime Victims Assistance Act in its entirety. In addition to the provisions that are included in today's antiterrorism package, this legislation provides for comprehensive reform of Federal law to establish enhanced rights and protections for victims of Federal crime. It also proposes several programs to help States provide better assistance for victims of State crimes. I also regret that we have not done more for other victims of recent terrorist attacks. While all Americans are numbed by the heinous acts of September 11th, we should not forget the victims of the 1998 embassy bombings in East Africa. Eleven Americans and many Kenyan and Tanzanian nationals employed by the United States lost their lives in that tragic incident. It is my understanding that compensation to the families of these victims has in many instances fallen short. It is my hope that OVC will use a portion of the newly replenished reserve fund to remedy any inadequacy that these individuals have been treated.

Hate crimes. We cannot speak of the victims of the September 11 without also noting that Arab-Americans and Muslims in this country have become the targets of hate crimes, harassment, and intimidation. I applaud the President for speaking out against and condemning such acts, and visiting a mosque to demonstrate by action that all Americans are embraced in this country. I also commend the FBI Director for his periodic reports on the number of hate crime incidents against Arab-American and Muslims that the FBI is aggressively investigating and making clear that this is taken seriously and will be punished.

The USA Act contains, in section 102, a sense of the Congress that crimes and discrimination against Arab and Muslims are condoned. Many of us would like to do more, and finally enact effective hate crimes legislation, but the Administration has asked that the debate on that legislation be postponed. One of my greatest regrets regarding the negotiations in this bill was the objections that prevented the Local Law Enforcement Enhancement Act, S. 625, from being included in the USA Act.

State and local law enforcement. The Administration's initial proposal was entirely focused on Federal law enforcement. Yet, we must remember that state and local law enforcement officers have critical roles to play in preventing and investigating terrorist acts. I am pleased that the USA Act we consider today recognizes this fact.

As a former State prosecutor, I know that State and local law enforcement officers are often the first responders to a crime. On September 11th, the nation saw that the first on the scene were the heroic firefighters, police officers and emergency personnel in New York City. These New York public safety officers, many of whom gave the ultimate sacrifice, remind us of how important it is to support our State and local law enforcement partners. The USA Act provides three critical measures of Federal support for our State and local law enforcement officers in the worldwide fight against terrorism.

First, we streamline and expedite the Public Safety Officers' Benefits application process for family members of fire fighters, police officers and rescue workers who perish or suffer a disabling injury in connection with prevention, investigation, rescue or recovery efforts related to a future terrorist attack.

The Public Safety Officers' Benefits Program provides benefits for each of the families of law enforcement officers, firefighters, and emergency response crew members who are killed or disabled in the line of duty. Current regulations, however, require the families of public safety officers who have fallen in the line of duty to go through a cumbersome and time-consuming application process. In the face of our national fight against terrorism, it is important that we provide a quick process to support those brave Americans who selflessly give their lives so that others might live before, during and after a terrorist attack. This provision builds on the new law championed by Senator Clinton, Senator Schumer and Congressman Nadler to speed the benefit payment process for families of public safety officers killed in the line of duty in New York City, Virginia, and Western Pennsylvania, on September 11.

Second, we have increased the total amount of Public Safety Officers' Benefits Program payments from approximately $150,000 to $250,000. This provision retroactively goes into effect to provide much-needed relief for the families of the brave men and women who sacrificed their own lives for their fellow Americans during the year. Although this increase in benefits can never replace a family's tragic loss, it is the right thing to do for the families of our fallen heroes. Thank you, Senator Biden and Senator Hatch for their bipartisan leadership on this provision.

Third, we expand the Department of Justice Regional Information Sharing Systems Program to promote information sharing among Federal, State and local law enforcement agencies to investigate and prosecute terrorist conspiracies and activities and authorize a doubling of funding for this year and next year. The RISS Program is a nationwide law enforcement network that already allows secure communications among the more than 5,700 Federal, State and local law enforcement agencies. Effective communication is key to effective law enforcement efforts and will be essential in our national fight against terrorism.

The RISS program enables its member agencies to send secure, encrypted communications—whether within just one agency or from one to another. Federal agencies, such as the FBI, do not have this capability, but recognize the need for it. Indeed, on September 11, 2001, immediately after the terrorist attacks, FBI Headquarters called RISS officials to request "Smartgate" cards and readers to secure their communications systems. The FBI agency in Philadelphia called soon after to request more "Smartgate" cards and readers as well.

The Regional Information Sharing Systems Program is a proven success that we need to expand to improve secure information sharing among Federal, State and local law enforcement agencies.
agencies to coordinate their counter-terrorism efforts.

Our State and local law enforcement partners welcome the challenge to join in our national mission to combat terrorism. We cannot ask State and local law enforcement officers to assume these new national responsibilities without also providing new Federal support. The USA Act provides the necessary Federal support for our State and local law enforcement officers to serve as full partners in our fight against terrorism.

I am deeply troubled by continuing reports that information is not being shared with state local law enforcement. In particular, the testimony of Baltimore Police Chief Ed Norris before the House Government Reform Committee last week highlighted the current problem.

Northern borders. The unfolding facts about how the terrorists who committed the September 11 attack were able to enter this country without difficulty are chilling. Since the attacks many have pointed to our northern border as vulnerable to the entry of future terrorists. This is not surprising when a simple review of the numbers shows that the northern border has been routinely short-changed in personnel. While the number of border patrol agents along the southern border has increased over the last few years, the number at the northern border remains the same as a decade ago at 300. This remains true despite the fact that Admad Ressam, the Algerian who planned to blow up the Los Angeles International Airport in 1999, and who has been linked to those involved in the September 11 attacks, chose to enter the United States at our northern border. It will remain an inviting target until we dramatically improve our security.

The USA Act includes my proposals to provide the substantial and long overdue assistance for our law enforcement and border control efforts along the Northern Border. My home state of Vermont has seen huge increases in customs and INS activity since the signing of NAFTA. The number of people coming through our borders has risen steeply over the years, but our staff and our resources have not.

I proposed—and this legislation authorizes in section 402—tripling the number of Border Patrol, INS Inspectors, and customs Service employees in each of the States along the 4,000-mile Northern Border. I was gratified when 22 Senators—Democrats and Republicans—wrote to the President supporting such an increase, and I am pleased that the Administration agreed that this critical law enforcement improvement should be included in the bill. Senators CANTWELL and SCHUMER in the Committee and Senators MURRAY and DORGAN have been especially strong in pressing these provisions and I thank them for their leadership.

In addition, the USA Act, in section 401, authorizes the Attorney General to waive the FTE cap on INS personnel in order to address the national security needs of the United States on the northern border. Now more than ever, we must patrol our border vigilantly and prevent those who wish America harm from traveling. At the same time, we must work with the Canadians to allow speedy crossing to legitimate visitors and foster the continued growth of trade which is beneficial to both countries.

In addition to providing for more personnel, this bill also includes, in section 402(4), my proposal to provide $100 million in funding for both the INS and the Customs Service to improve the technology to monitor the Northern Border and to purchase additional equipment. The bill also includes, in section 403(c), an important provisions from Senator CANTWELL directing the Attorney General, in consultation with Customs Service, to develop a technical standard for identifying electronically the identity of persons applying for visas or seeking to enter the United States. In short, this bill provides a comprehensive high-tech boost for the security of our Nation.

This bill also includes important proposals to enhance data sharing. The bill, in section 403, directs the Attorney General and the FBI Director to give the State Department and INS access to the criminal history information in the FBI’s National Crime Information Center (NCIC) database, as the Administration and I both proposed. The Attorney General is directed to report back to the Congress in two years on progress in implementing this requirement. We have also adopted the Administration’s language, in section 413, to make it easier for the State Department to share information with foreign governments to aid in terrorist investigations.

Criminal justice improvements. The USA Act contains a number of provisions intended to improve and update the federal criminal code to address terrorism, recent terrorist attacks, and assist the FBI in translating foreign language information collected, and ensure that federal prosecutors are unhindered by conflicting local rules of conduct to get the job done. I will mention just a few of these provisions.

FBI translators. The truth certainly seems self-evident that all the best surveillance techniques in the world will not help this country defend itself from terror unless the information cannot be understood in a timely fashion. Indeed, within days of the September 11, the FBI Director issued an employment ad on national TV by calling upon those who speak Arabic to apply for a job as a translator. This is a dire situation that needs attention. I am therefore gratified that the Administration accepted my proposal, in section 265, to waive any federal personnel requirements and limitations imposed by any other law in order to expedite the hiring of translators at the FBI.

This bill also directs the FBI Director to establish such security requirements as are necessary for the personnel employed as translators. We know the effort to recruit translators has a high priority, and the Congress should provide all possible support. Therefore, the bill calls on the Attorney General to report to the Judiciary Committees on the number of translators employed by the Justice Department, any legal or practical impediments to using translators employed by other Federal, State, or local agencies on a full, part-time, or shared basis; and the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

Federal crime of terrorism. The Administration’s initial proposal assemblers a laundry list of more than 40 Federal crimes ranging from computer hacking to malicious mischief to the use of weapons of mass destruction, and penalties. The maximum penalties would shoot up to life imprisonment, and those released earlier would be subject to a lifetime of supervised release. Moreover, anyone who harbored a person whom he had “reason to believe” was guilty of terrorism offenses, would be deemed to have committed this new “terrorism” offense. Under the Administration’s proposal, the consequences of this designation were severe. Crimes on the list would carry no statute of limitations. The maximum penalties would shoot up to life imprisonment, and those released earlier would be subject to a lifetime of supervised release. Moreover, anyone who harbored a person whom he had “reasonable grounds to suspect” had committed, or was about to commit, a “Federal terrorism offense”—whether it was the Taliban or the mother of my hypothetical teenage computer hacker—would be subject to stiff criminal penalties.

Therefore, the bill calls on the Administration to ensure that the definition of “terrorism” in the USA Act fit the crime.

First, we have trimmed the list of crimes that may be considered as terrorism offenses in the USA Act, and designated them as terrorism offenses, on a full, part-time, or shared basis; and the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

Second, we have provided, in section 810, that the current 8-year limitations period for this new set of offenses will remain in place, except where the commission of the offense resulted in, or created a risk of, death or serious bodily injury. Then, rather than make an across-the-board, one-size-fits-all increase of the penalties for every offense on the list, without regard to the severity of the offense, we have made, in section 811, the list a hypothetical teenage computer hacker to malicious mischief to the use of weapons of mass destruction, and those released earlier would be subject to a lifetime of supervised release. Moreover, anyone who harbored a person whom he had “reasonable grounds to suspect” had committed, or was about to commit, a “Federal terrorism offense”—whether it was the Taliban or the mother of my hypothetical teenage computer hacker—would be subject to stiff criminal penalties.

Third, we have provided, in section 810, that the current 8-year limitations period for this new set of offenses will remain in place, except where the commission of the offense resulted in, or created a risk of, death or serious bodily injury. Third, rather than make an across-the-board, one-size-fits-all increase of the penalties for every offense on the list, without regard to the severity of the offense, we have made, in section 811, the list a hypothetical teenage computer hacker to malicious mischief to the use of weapons of mass destruction, and those released earlier would be subject to a lifetime of supervised release. Moreover, anyone who harbored a person whom he had “reasonable grounds to suspect” had committed, or was about to commit, a “Federal terrorism offense”—whether it was the Taliban or the mother of my hypothetical teenage computer hacker—would be subject to stiff criminal penalties.
Finally, we have more carefully defined the new crime of harboring terrorists in section 804, so that it applies only to those harboring people who have committed, or are about to commit, the most serious of federal terrorism-related crimes, such as the acquisition of weapons of mass destruction. Moreover, it is not enough that the defendant had “reasonable grounds to suspect” that the person he was harboring had committed, or was about to commit, such a crime; the government must prove that the defendant knew or had “reasonable grounds to believe” that this was so.

McDade fix. The massive investigation underway into who was responsible for and assisted in carrying out the September 11 attacks stretches across state and national boundaries. While the scope of the tragedy is unsurpassed, the disregard for state and national borders of this criminal conspiracy is not unusual. Federal investigators and prosecutors must follow leads and conduct investigations outside their assigned jurisdictions. At the end of the 105th Congress, a legal impediment to such multi-jurisdictional investigations was lifted when the Senate approved the McDade bill, over the objection at the time of every member of the Senate Judiciary Committee.

I have spoken many times over the past two years of the problems caused by the earlier McDade law, 28 U.S.C. § 530B. According to the Justice Department, the McDade law has delayed important criminal investigations, prevented the use of effective and traditionally accepted investigative techniques, and served as the basis of litigation to interfere with legitimate federal prosecutions. At a time when we need federal law enforcement authorities to move quickly to catch those responsible for the September 11th attacks, and to prevent further attacks on our country, we can no longer tolerate the drag on federal investigations and prosecutions caused by this ill-considered legislation.

On September 19th, I introduced S. 1437, the Professional Standards for Government Attorneys Act of 2001, along with Senators HATCH and WYDEN. This bill proposes to modify the McDade law by establishing a set of rules that clarify the professional standards for government attorneys. I am delighted that the Administration recognized the importance of S. 1437 for improving federal law enforcement and combating terrorism, and agreed to its inclusion as section 501 of the USA Act.

The first part of section 501 embodies the traditional understanding that when lawyers handle cases before a Federal court, they should be subject to the Federal court’s standards of professional responsibility, and not to the possibility of lesser standards of other jurisdictions. By incorporating this ordinary choice-of-law principle, the bill preserves the Federal courts’ traditional authority to oversee the professional conduct of Federal trial lawyers, including Federal prosecutors. It thus avoids the uncertainties presented by the McDade law, which potentially subjects Federal prosecutors to State court requirements for criminal procedure, and judicial decisions which differ from existing Federal law.

Another part of section 501 specifically addresses the situation in Oregon, where a state court ruling has seriously impeded the ability of Federal agents to engage in undercover operations and other covert activities. See In re Gatti, 330 Or. 517 (2000). Such activities are legitimate and essential crime-fighting tools. The Professional Standards for Government Attorneys Act ensures that these tools will be available to combat terrorism.

Finally, section 501 addresses the most pressing contemporary question of government attorney ethics—namely, the question of which rule should govern government attorneys’ communications with represented persons. It asks the Judicial Conference of the United States to submit to the Supreme Court a proposed uniform national rule to govern this area of professional conduct. To study the need for additional national rules to govern other areas in which the proliferation of local rules may interfere with effective Federal law enforcement.

The Rules Enabling Act process provides the mechanism for developing such rules, both because the Federal judiciary traditionally is responsible for overseeing the conduct of lawyers in Federal court proceedings, and because this process would best provide the Supreme Court an opportunity fully to consider and objectively to weigh all relevant considerations.

The problems posed to Federal law enforcement investigators and prosecutors by the McDade law are real and very serious. The Professional Standards for Government Attorneys Act provides a reasonable and measured alternative: It preserves the traditional role of the State courts in regulating the conduct of attorneys licensed to practice before them, while ensuring that Federal prosecutors and law enforcement agents will be able to use traditional Federal investigative techniques. We need to pass this corrective legislation before more cases are compromised.

Terrorist attacks against mass transportation systems. Another provision of the USA Act that was not included in the Administration’s initial proposal is section 801, which targets acts of terrorism and other violence against mass transportation systems. Just last week, a Greyhound bus crashed in Tennessee after a deranged passenger slit the driver’s throat and then grabbed the steering wheel, force the bus into oncoming traffic. Six people were killed in the crash. Before there are currently no federal law addressing terrorism of mass transportation systems, however, there may be no federal jurisdiction over such cases, even if it were committed by suspected terrorists. Clearly, there is an urgent need for strong criminal legislation to deter attacks against mass transportation systems. Section 801 will fill this gap.

Cybercrime. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is the federal primary criminal statute prohibiting computer frauds and hacking. I worked with Senator HATCH in the last Congress to make improvements to this law in the Internet Security Act, which passed the Senate as part of another bill. Our work is included in section 815 of the USA Act. This section would amend the statute to clarify the appropriate scope of federal jurisdiction. First, the bill adds a definition of “loss” to cover any reasonable cost to the victim in responding to a computer hacker. Calculation of loss is important both in determining whether the $5,000 jurisdictional hurdle in the statute is met, and, at sentencing, in calculating the appropriate guideline range and restitution amount.

Second, the bill amends the definitions of “protected computer” to include any computer, or any facilities, equipment, and supplies of which they are physically located outside of the United States. This clarification will preserve the ability of the United States to assist in internal hacking cases.

Finally, this section eliminates the current directivity of the Sentencing Commission requiring that for violations, including misdemeanor violations, of certain provisions of the Computer Fraud and Abuse Act be punished with a term of imprisonment of at least six months.

Biological weapons. Borrowing from a bill introduced in the last Congress by Senator BIDEN, the USA Act contains a provision in section 802 to strengthen our federal laws relating to the threat of biological weapons. Current law prohibits the possession, development, or acquisition of biological agents or toxins “for weaponization.” This section amends the definition of “for weaponization” to include all situations in which it can be proven that the defendant had any purpose other than a peaceful purpose. This will enhance the government’s ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. § 175 more closely to the related forfeiture provision in 18 U.S.C. § 176. This section also contains a new statute, 18 U.S.C. § 175b, which generally makes it an offense for certain restricted persons, including non-resident aliens from countries that support international terrorism, to possess a listed biological agent or toxin.

Of greater consequence, section 802 defines another additional offense, punishable by up to 10 years in prison, of possessing a biological agent, toxin, or delivery system “of a type or in a
Section 507 of the USA Act gives the Secret Service concurrent jurisdiction to investigate offenses under 18 U.S.C. § 1030, relating to fraud and related activity in connection with computers. Prior to the 1996 amendments to the Computer Fraud and Abuse Act, the Secret Service was authorized to investigate Internet fraud crimes under section 1030, pursuant to an agreement between the Secretary of Treasury and the Attorney General. The 1996 amendments, however, concentrated Secret Service jurisdiction on certain specified computer fraud crimes, and thus the current amendment would return full jurisdiction to the Secret Service and would allow the Justice and Treasury Departments to decide on the appropriate work-sharing balance between the two.

This amendment would allow the Secret Service to investigate a wide range of potential White House network intrusions, as well as intrusions into remote sites (outside of the White House) that could impact the safety and security of the nation’s critical infrastructure and financial payment systems.

Counter-terrorism Fund. The USA Act also authorizes, for the first time, a counter-terrorism fund in the Treasury of the United States to reimburse Justice Department for any costs incurred in connection with the fight against terrorism. Specifically, this counter-terrorism fund will: (1) reestablish an office or facility that has been damaged as the result of any domestic or international terrorism incident; (2) provide support to counter, investigate, or prosecute domestic or international terrorism, including paying rewards in connection with these activities; (3) conduct terrorism threat assessments of Federal agencies; and (4) for costs incurred in connection with detaining individuals who are accused of acts of terrorism in violation of United States law.

I first authored this counter-terrorism fund in the S. 1319, the 21st Century Department of Justice Appropriations Authorization Act, which Senator HATCH and I introduced in August.

Enhanced surveillance procedures. The USA Act provides enhanced surveillance procedures for the investigation of terrorism and other crimes. This challenge before us has been to strike a reasonable balance to protect both security and the liberties of our people. In some respects, the changes made are appropriate and important ones to update surveillance investigative procedures in light of new technology and experience with current law. Yet, in other respects, I have deep concerns that we may be increasing surveillance powers and the sharing of criminal justice information without adequate checks on how information may be handled and without adequate accountability in the form of judicial review.

The bill contains a number of sensible proposals that should not be controversial. Wiretap predicates. For example, sections 201 and 202 of the USA Act would add to the list of crimes that may be used as predicates for wiretaps certain offenses which are specifically tailored to the terrorist threat. In addition to crimes that relate directly to terrorism, the list would include crimes of espionage, which are committed by terrorists to support and advance their illegal objectives.

FISA roving wiretaps. The bill, in section 206, would authorize the use of roving wiretaps in the course of a foreign Intelligence investigation and brings FISA into line with criminal procedures that allow surveillance to follow a person, rather than requiring a separate court order identifying each telephone company or other communication common carrier whose assistance is needed. This is a matter on which the Attorney General and I reached early agreement. This is the kind of change that has a compelling justification, because it recognizes the ease with which targets of investigations can evade surveillance by changing phones. In fact, the original roving wiretap authority for use in criminal investigations was enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986. I was proud to be the primary Senate sponsor of that earlier law.

Paralleling the statutory rules applicable to criminal investigations, the formulation I originally proposed made clear that this new wiretap authority must be requested in the application before the FISA court was authorized to order such roving surveillance authority. Indeed, the Administration agrees that the FISA court may not grant such authority sua sponte. Nevertheless, we have accepted the Administration’s formulation of the new roving wiretap authority, which requires the FISA court to make a finding that the actions of the person whose communications are to be intercepted are so connected with the identification of a specified facility or place. While no amendment is made to the statutory directions for what must be included in the application for a FISA electronic surveillance order, these applications should include the necessary information to support the FISA court’s finding that roving wiretap authority is warranted.

Search warrants. The USA Act, in section 219, authorizes nationwide service of judicial search warrants in terror investigations. This will allow the judge who is most familiar with the developments in a fast-breaking and complex terrorism investigation to make determinations of probable cause, no matter where the property to be searched is located. This will not only save time by avoiding having to bring up-to-speed another judge in another jurisdiction where the property is located, but also serves privacy and Fourth Amendment interests in ensuring that the most knowledgeable judge makes the determination of probable cause. The bill, in section 209, also authorizes voice mail messages to be seized on the authority

quantity that, under the circumstances,” is not reasonably justified by a peaceful purpose. As originally proposed by the Administration, this provision specifically stated that knowledge of whether the type or quantity of the act was peaceful or terrorist in nature was not an element of the offense. Thus, although the burden of proof is always on the government, every person who possesses a biological agent, toxin, or delivery system was at some level of threshold treated as guilty if the possession was not reasonably justified. I am pleased that the Administration agreed to drop this portion of the provision.

Nevertheless, I remain troubled by the subjectivity of the substantive standard for violation of this new criminal prohibition, and question whether it provides sufficient notice under the Constitution. I also share the concerns of the American Society for Microbiology and the Association of American Universities that this provision will have a chilling effect upon legitimate research that serves any benefit in protecting against terrorism. While we have tried to prevent against this by creating an explicit exclusion for “bona fide research,” this provision may yet prove unworkable, uncertain, or both. I urge the Justice Department and the research community to work together on substitute language that would provide prosecutors with a more workable tool.

The Secret Service is committed to the development of new tools to combat the changing threats of terrorism and computer crime, computer fraud, and cyberterrorism. Recognizing a need for law enforcement, private industry and academia to pool their resources, skills and revision to combat criminal elements in cyberspace, the Secret Service created the New York Electronic Crimes Task Force (NYECTF). This highly successful model is comprised of over 250 individual members, including 50 different Federal, State and local enforcement agencies; 100 private companies, and 9 universities. Since its inception in 1995, the NYECTF has successfully investigated a range of financial and electronic crimes, including credit card fraud, identify theft, bank fraud, computer systems intrusions, and e-mail threats against protectees of the Secret Service. Section 105 of the USA Act authorizes the Secret Service to develop similar task forces in cities and regions across the country where critical infrastructure may be vulnerable to attacks from terrorists or other cyber-criminals.

Section 507 of the USA Act gives the Secret Service concurrent jurisdiction to investigate offenses under 18 U.S.C. §1030, relating to fraud and related activity in connection with computers. Prior to the 1996 amendments to the Computer Fraud and Abuse Act, the Secret Service was authorized to investigate Internet fraud crimes under section 1030, pursuant to an agreement between the Secretary of Treasury and the Attorney General. The 1996 amendments, however, concentrated Secret Service jurisdiction on certain specified computer fraud crimes, and thus the current amendment would return full jurisdiction to the Secret Service and would allow the Justice and Treasury Departments to decide on the appropriate work-sharing balance between the two.

This amendment would allow the Secret Service to investigate a wide range of potential White House network intrusions, as well as intrusions into remote sites (outside of the White House) that could impact the safety and security of the nation’s critical infrastructure and financial payment systems.

Counter-terrorism Fund. The USA Act also authorizes, for the first time, a counter-terrorism fund in the Treasury of the United States to reimburse Justice Department for any costs incurred in connection with the fight against terrorism.

Specifically, this counter-terrorism fund will: (1) reestablish an office or facility that has been damaged as the result of any domestic or international terrorism incident; (2) provide support to counter, investigate, or prosecute domestic or international terrorism, including paying rewards in connection with these activities; (3) conduct terrorism threat assessments of Federal agencies; and (4) for costs incurred in connection with detaining individuals who are accused of acts of terrorism in violation of United States law.

I first authored this counter-terrorism fund in the S. 1319, the 21st Century Department of Justice Appropriations Authorization Act, which Senator HATCH and I introduced in August.

Enhanced surveillance procedures. The USA Act provides enhanced surveillance procedures for the investigation of terrorism and other crimes. This challenge before us has been to strike a reasonable balance to protect both security and the liberties of our people. In some respects, the changes made are appropriate and important ones to update surveillance investigative procedures in light of new technology and experience with current law. Yet, in other respects, I have deep concerns that we may be increasing surveillance powers and the sharing of criminal justice information without adequate checks on how information may be handled and without adequate accountability in the form of judicial review.

The bill contains a number of sensible proposals that should not be controversial. Wiretap predicates. For example, sections 201 and 202 of the USA Act would add to the list of crimes that may be used as predicates for wiretaps certain offenses which are specifically tailored to the terrorist threat. In addition to crimes that relate directly to terrorism, the list would include crimes of espionage, which are committed by terrorists to support and advance their illegal objectives.

FISA roving wiretaps. The bill, in section 206, would authorize the use of roving wiretaps in the course of a foreign Intelligence investigation and brings FISA into line with criminal procedures that allow surveillance to follow a person, rather than requiring a separate court order identifying each telephone company or other communication common carrier whose assistance is needed. This is a matter on which the Attorney General and I reached early agreement. This is the kind of change that has a compelling justification, because it recognizes the ease with which targets of investigations can evade surveillance by changing phones. In fact, the original roving wiretap authority for use in criminal investigations was enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986. I was proud to be the primary Senate sponsor of that earlier law.

Paralleling the statutory rules applicable to criminal investigations, the formulation I originally proposed made clear that this new wiretap authority must be requested in the application before the FISA court was authorized to order such roving surveillance authority. Indeed, the Administration agrees that the FISA court may not grant such authority sua sponte. Nevertheless, we have accepted the Administration’s formulation of the new roving wiretap authority, which requires the FISA court to make a finding that the actions of the person whose communications are to be intercepted are so connected with the identification of a specified facility or place. While no amendment is made to the statutory directions for what must be included in the application for a FISA electronic surveillance order, these applications should include the necessary information to support the FISA court’s finding that roving wiretap authority is warranted.

Search warrants. The USA Act, in section 219, authorizes nationwide service of judicial search warrants in terror investigations. This will allow the judge who is most familiar with the developments in a fast-breaking and complex terrorism investigation to make determinations of probable cause, no matter where the property to be searched is located. This will not only save time by avoiding having to bring up-to-speed another judge in another jurisdiction where the property is located, but also serves privacy and Fourth Amendment interests in ensuring that the most knowledgeable judge makes the determination of probable cause. The bill, in section 209, also authorizes voice mail messages to be seized on the authority
of a probable cause search warrant rather than through the more burdensome and time-consuming process of a wiretap.

Electronic records. The bill updates the laws pertaining to electronic records in three primary ways. First, in section 210, the bill authorizes the nationwide service of subpoenas for subscriber information and expands the list of items subject to subpoena to include the means and source of payment for the service.

Second, in section 211, the bill equalizes the standard for law enforcement access to cable subscriber records on the same basis as other electronic records. The Cable Communications Privacy Act, passed in 1984 to regulate various aspects of the cable television industry, did not take into account the changes in technology that have occurred over the last fifteen years. Cable television companies now often provide Internet and telephone services in addition to television programming. This amendment clarifies that a cable company must comply with the laws governing the interception and disclosure of wire and electronic communications just like any other telephone company or Internet service provider. The amendments would retain current standards that govern the release of customer records for television programming.

Finally, the bill, in section 212, permits, but does not require, an electronic communications service to disclose the contents of and subscriber information about communications in emergencies involving the immediate danger of death or serious physical injury. Under current law, if an ISP’s customer receives an e-mail death threat from another customer of the same ISP, and the victim provides a copy of the communication to the ISP, the ISP is limited in what actions it may take. On one hand, the ISP may disclose the contents of the forwarded communication to law enforcement (or to any other third party as it sees fit) See 18 U.S.C. § 2702(b)(3). On the other hand, current law does not expressly authorize the ISP to voluntarily provide law enforcement with the identity, home address, and other subscriber information of the user making the threat. See 18 U.S.C. § 2703(c)(1)(B), (C) (permitting disclosure to governmental entities for the purpose of responding to a legal process). In those cases where the risk of death or injury is imminent, the law should not require providers to sit idly by. This voluntary disclosure, however, in no way creates additional legal obligations for customers or telecommunications carriers in search of such imminent dangers.

Also, under existing law, a provider (even one providing services to the public) may disclose the contents of a customer’s communications—law enforcement or anyone else—in order to protect its rights or property. See 18 U.S.C. § 2702(b)(5). However, the current statute does not expressly permit a provider voluntarily to disclose non-content records (such as a subscriber’s login records) to law enforcement for purposes of self-protection. See 18 U.S.C. § 2703(c)(1)(B). Yet the right to disclose the content of communications is not an absolute intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company’s authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter providers must have the right to disclose the facts surrounding attacks on their systems. When a telephone carrier is defrauded by a subscriber, or when an ISP’s authorized user launches a network intrusion against his own ISP, the provider must have the legal ability to report the crime to law enforcement. The bill clarifies that service providers have the statutory authority to make such disclosures.

Pen registers. There is consensus that the existing legal procedures for pen register and trap-and-trace authority are antiquated and need to be updated. I have been proposing ways to update the pen register and trap and trace statutes for several years, but not necessarily in the same ways as the Administration initially proposed. In fact, in 1998, I introduced with then-Senator Ashcroft, the E-PRIVACY Act, S. 2067, which proposed changes in the pen register laws. In 1999, I introduced the E-RIGHTS Act, S. 934, also with proposals to update the pen register laws.

Again, in the last Congress, I introduced the Internet Security Act, S. 2430, on April 13, 2000, that proposed (1) another version of a pen register and trap device law to give nationwide effect to pen register and trap and trace orders obtained by Government attorneys and obviate the need to obtain identical orders in multiple federal jurisdictions; (2) clarifying that such devices can be used for computer transmissions to obtain electronic addresses, not just on telephone lines; and (3) as a guard against abuse, providing for meaningful judicial review of government attorney applications for pen registers and trap and trace devices.

As the outline of my earlier legislation suggests, I have long supported modernizing the pen register and trap and trace device laws by modifying the statutory language to cover the use of these orders on computer transmissions; to remove the jurisdictional limits on service of these orders; and to update the judicial review procedure, which, unlike any other area in criminal procedure, bars the exercise of judicial discretion in the just identification for the order. The USA Act, in section 216, updates the pen register and trap and trace laws only in two out of three respects I believe are important, and without allowing meaningful judicial review. Yet, we were able to improve the Administration’s initial proposal, which suffered from the same problem as the provision that was hastily and passed by the Senate, by voice vote, on September 13, 2001, as an amendment to the Commerce Justice State Appropriations Act.

Nationwide service. The existing legal procedures for pen register and trap-and-trace authority require the service of individual orders for installation of pen register or trap and trace device on the service providers that carried the targeted communications. Deregulation of the telecommunications industry has had the consequence that one communication may be carried by multiple providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it at a switch to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to an incumbent local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not provide service information with each call, identifying that call, they require compelling information from a host of providers located throughout the country.

Under present law, a court may only authorize the installation of a pen register or trap device “within the jurisdiction of the court.” As a result, when one provider indicates that the source of a communication is a carrier in another district, a second order may be necessary. The Department of Justice has advised, for example, that in 1996, a hacker (who later turned out to be launching his attacks from a foreign country) extensively penetrated computers belonging to the Department of Defense. This hacker was dialing into a host at Harvard University and used this computer as an intermediate staging point in an effort to conceal his location and identity. Investigators obtained a trap and trace order instructing the phone company, Nynex, to trace these calls, but Nynex could only report that the communications were coming to it from a long-distance carrier, MCI. Investigators then applied for a court order to obtain the connection information from MCI, but since Nynex was not authorized to supply this using the connection, MCI could not identify its source. Only if the investigators could have served MCI with a trap and trace order while the hacker was actively on-line could they have successfully traced back and located him.

In another example provided by the Department of Justice, investigators encountered similar difficulties in attempting to track Kevin Mitnick, a criminal who continued to hack into computer networks throughout the Internet despite the fact that he was on supervised release for a prior computer crime conviction. The FBI attempted to trace
these electronic communications while they were in progress. In order to evade arrest, however, Mitnick moved around the country and used cloned cellular phones and other evasive techniques. His hacking attacks would often pass through one or more cellular carriers to reach the intended target, only to be decoded by the local phone company and two Internet service providers. In this situation, where investigators and service providers had to act quickly to trace Mitnick in the act of hacking, only many repeated attempts—accompanied by an enormous service charge—finally produced success. Fortunately, Mitnick was such a persistent hacker that he gave law enforcement many chances to complete the trace.

This duplicative process of obtaining a separate order for each link in the communications chain can be quite time-consuming, and it serves no useful purpose since the original court has already authorized the trace. Moreover, a second or third order addressed to a service provider that carried part of a prior communication may prove useless during the next attack: in computer intrusion cases, for example, the target may use an entirely different path (i.e., utilize a different set of intermediate providers) for his or her subsequent activity.

The bill would modify the pen register and trap and trace statutes to allow for nationwide service of a single order for installation of these devices, without the necessity of returning to court for each new carrier. I support this change.

Second, the language of the existing statute is hopelessly out of date and speaks of a pen register or trap and trace “device” being “attached” to a telephone “line.” However, the rapid computerization of the telephone system has changed the tracing process. No longer are such functions normally accomplished by physical hardware components attached to telephone lines. Instead, these functions are typically performed by computerized collection and retention of call routing information passing through a communications system.

The statute’s definition of a “pen register” as a “device” that is “attached” to a particular “telephone line” is particularly obsolete when applied to the wireless portion of a cellular phone call, which has no line to which anything can be attached. While courts have authorized pen register orders for wireless phones based on the notion of obtaining access to a “virtual line,” updating the law to keep pace with current technology is a better course.

Moreover, the statute is ill-equipped to facilitate the tracing of communications that take place over the Internet. For example, the pen register definition refers to telephone “numbers” rather than the broader concept of a user’s communications account. Although pen register and trap orders have been obtained for activity on computer networks, Internet service providers have challenged the application of the statute to electronic communications, frustrating legitimate investigations. I have long supported updating the statute by removing words such as “numbers . . . dialed” that do not apply when non-wire devices are used and to clarify the statute’s proper application to tracing communications in an electronic environment, but in a manner that is technology neutral and does not capture the content of communications. That is precisely what I am being, I have been concerned about the FBI and Justice Department’s insistence over the past few years that the pen/trap devices statutes be updated with broad, undefined terms that continue to flame concerns that these laws will be used to intercept private communications content.

The Administration’s initial pen/trap device proposal added the terms “routing” and “addressing” to the definitions describing the information that was authorized for interception on the low relevance standard under these laws. The Administration and the Department of Justice flatly rejected my suggestion that these terms be defined to respond to concerns that the new technologies might consis- tently contain information that may be captured only upon a showing of probable cause, not the mere relevancy of the pen/trap statute. Instead, the Administration agreed that the definition should explicitly describe pen/trap de- vices to intercept “content,” which is broadly defined in 18 U.S.C. 2510(8).

While this is an improvement, the FBI and Justice Department are short- sighted in their refusal to define these terms. We should be clear about the consequence of not providing definitions for these new terms in the pen/ trap device statutes. These terms will be defined, if not by the Congress, then by the courts in the context of crimi- nal investigations that have been used and challenged by defend- ants. If a court determines that a pen register has captured “content,” which the FBI admits such devices do, in viola- tion of the Fourth Amendment, suppression may be ordered, not only of the pen register evidence but any other evidence derived from it. We are leaving the courts with little or no guidance of what is covered by “addressing” or “routing.”

The bill also requires the gov- ernment to use reasonably available technology that limits the intercep- tions under the pen/trap device laws “so as not to include the contents of any wire or electronic communica- tions.” This limitation on the tech- nology used by the government to exe- cute pen/trap orders is important since, as the FBI advised me June, 2000, pen register devices “do capture all elec- tronic impulses transmitted by the facili- ty on which they are attached, including those transmitted after the call is connected to the called party.” The impulses made after the call is connected could reflect the electronic banking transactions a caller makes, or the electronic ordering from a catalogue that a customer makes over the telephone, or the elec- tronic ordering of a prescription drug.

This transactional data intercepted after the call is connected is the “con- tent.” As the Justice Department explained in May, 1998 in a letter to House Judiciary Committee Chairman Henry Hyde, “the retrieval of the elec- tronic impulses that a caller neces- sarily generated in attempting to di- rect the phone call” does not con- stitute a “search” requiring probable cause since “no part of the substantive information transmitted after the caller had reached the called party” is ob- tained. But the Justice Department made clear that “all of the information transmitted after a phone call is con- nected to the called party . . . is sub- stantive in nature. These electronic impulses are the ‘contents’ of the call: They are not used to direct or process the call but instead convey certain messages to the recipient.”

When I added the direction on use of reasonably available technology (codi- fied as 18 U.S.C. 3121(c)) to the pen reg- ister statute as part of the Commu- nications Assistance to Law Enforcement Act (CALEA) in 1994, I recognized that these devices collected content and that such collection was unconsti- tutional on the mere relevance standard. Nevertheless, the FBI advised me in June, 2000, that pen register devices for telephone services “continue to op- erate as they have for decades” and that “there had been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call proc- essing.” Perhaps, if there were mean- ingful judicial review and account- ability, the FBI would take the statu- tory direction more seriously and actu- ally implement it.

Judicial review. Due in significant part to the fact that pen/trap devices in use today collect “content,” I have sought in legislation introduced over the past few years to update and mod- ify the judicial review procedure for pen register and trap and trace devices. Existing law requires an attorney for the government to certify that the information likely to be obtained by the installation of a pen register or trap and trace device will do an ongoing criminal investigation. The court is required to issue an order upon seeing the prosecutor’s certification. The court is not authorized to look be- hind the certification to evaluate the judgment of the prosecutor. I have urged that government attor- neys be required to include facts about their investigations in their applica- tions for pen/trap orders and allow courts to grant such orders only where the facts support the relevancy of the information likely to be obtained by the orders. This is not a change in the applicable standard, which would re- main the very low relevancy standard.
Instead, this change would simply allow the court to evaluate the facts presented by a prosecutor, and, if it finds that the facts support the government’s assertion that the information to be collected will be relevant, issue the order. In this change, it is feared, it place an additional burden on law enforcement, it will allow the courts a greater ability to assure that government attorneys are using such orders properly.

Some have called this change a “roll
[25x20]back” in the statute, as if the concept of allowing meaningful judicial review was an extreme position. To the contrary, this is a change that the Clinton Administration supported in legislation transmitted to the Congress last year. This is a change that the House Judiciary Committee also supported last year. In the Electronic Communications Privacy Act, H.R. 5018, that Committee proposed that before a pen/trap can be ordered for the investigation of any person, the government must first demonstrate to an independent judge that “specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such surveillance and use . . . is relevant to an investigation of that crime.” (Report 106-932, 106th Cong. 2d Sess., Oct. 4, 2000, p. 13).

Unfortunately, the Bush Administration has taken a contrary position and has rejected this change in the judicial review process.

Computer trespasser. Currently, an owner or operator of a computer that is accessed by a hacker as a means for the hacker to reach a third computer, cannot simply consent to law enforcement monitoring of the computer. Instead, because the owner or operator is not technically a party to the communications, law enforcement needs wiretap authorization under Title III to conduct such monitoring. I have long been interested in the loophole left by this legislation. In June 2000, when I asked about this problem, the FBI explained to me in June, 2000, that:

“This anomaly in the law creates an untenable situation whereby providers are sometimes forced to sit idly by as they witness hackers enter and, in some situations, destroy or damage their systems and networks while law enforcement begins the detailed investigation of that crime.

I therefore introduced as part of the Internet Security Act, S. 2430, in 2000, an exception to the wiretap statute that would explicitly permit such monitoring without a wiretap if prior consent is obtained from the person whose computer is being hacked through and used to send “harmful interference to a lawfully operating computer system.”

The Administration initially proposed a different formulation of the exception that would have allowed an owner/operator of any computer connected to the Internet to consent to FBI wiretapping of any user who violated a workplace computer use policy or online service term of service and was thereby an “unauthorized” user. The Administration’s proposal was not limited to computer hacking offenses under 18 U.S.C. 1030 or to conduct that caused harm to a computer system. The Administration rejected these refinements to their proposed wiretap exception, but did agree, in section 217 of the USA Act, to limit the authority for wiretapping with the consent of the owner/operator to communications of unauthorized users without an existing subscriber or other contractual relationship with the owner/operator.

Sharing criminal justice information. The USA Act will make significant changes in the sharing of confidential criminal justice information with various Federal agencies. For those of us who have been concerned about the leaks from the FBI that can irreparably damage reputations of innocent people investigating computer crimes by alerting suspects to flee or destroy material evidence, the Administration’s insistence on the broadest authority to disseminate such information, without any judicial check, is disturbing. Nonetheless, I believe we have improved the Administration’s initial proposal in responsible ways. Only time will tell whether the improvements we were able to reach agreement on are sufficient.

At the end of the day, we should be clear that current law allows the sharing of confidential criminal justice information, but with close court supervision. Federal Rule of Criminal Procedure 6(e) provides that matters occurring before a grand jury may be disclosed only to an attorney for the government, such other government personnel as are necessary to assist the attorney and another grand jury. Further disclosure is also allowed as specifically authorized by a court.

Similarly, section 2517 of title 18, United States Code provides that wiretap evidence may be disclosed in testimony during official proceedings and to investigative or law enforcement officers in the performance of their duties. In addition, the wiretap law allows disclosure of wiretap evidence “relating to offenses other than specified in the order when authorized or required by a neutral and detached judge.” Indeed, just last year, the Justice Department assured us that “law enforcement agencies have authority under current law to share title III information regarding terrorism with intelligence agencies when the information is of overriding importance to the national security.” (Letter from Robert Raben, Assistant Attorney General, September 28, 2000).

For this reason, and others, the Justice Department at the time opposed an amendment proposed by Senators KYL and FEINSTEIN to S. 2507, the “Intelligence Authorization Act for FY 2001 that would have allowed the sharing of foreign intelligence and counterintelligence information collected from wiretaps with the intelligence community. I deferred to the Justice Department on this issue and sought changes in the proposed amendment to address the Department’s concern that this proposal was not only unnecessary but also “could have significant implications for prosecutions and the discovery process in litigation”, “raises significant issues regarding the sharing with intelligence agencies of information” selected about United States persons and jeopardized “the need to protect equities relating to ongoing criminal investigations.” In the end, the amendment was revised to address the Justice Department’s concerns and passed the Senate as a free-standing bill, S. 3205, the Counterterrorism Act of 2000. The House took no action on this legislation.

Disclosure of wiretap information. The Administration initially proposed adding a sweeping provision to the wiretap statute that broadened the definition of an “investigative or law enforcement officer” who may receive disclosures of information obtained through wiretaps to include federal law enforcement, intelligence, national security, national defense, and immigration personnel and the President and Vice President. This proposal troubled me because information intercepted by a wiretap has enormous potential to infringe upon the privacy of innocent people who are not even suspected of a crime and merely happen to speak on the telephone with the targets of an investigation. For this reason, the authority to disclose information obtained through a wiretap has always been carefully circumscribed in law.

While I recognize that appropriate officials in the executive branch of government should have access to wiretap information that is important to combating terrorism or national security, I proposed allowing such disclosures where specifically authorized by a court order. Further, with respect to information relating to terrorism, I proposed allowing the disclosure without a court order as long as the judge who authorized the wiretap was notified as soon as practicable after the fact. This would have provided a check against abuses of the disclosure authority by providing for reviewing secret wiretaps with the judiciary. At the same time, there was a little likelihood that a judge would deny any requests for disclosure in cases where it was warranted.

On Sunday, September 30, the Administration agreed to my proposal, but within two days, it backed away from its agreement. I remain concerned that the resulting provision will allow the unprecedented, widespread disclosure of this highly sensitive information without any notification to the courts or the telephone companies, and supervises the wiretap. This is clearly an area where our Committee will have to exercise close oversight to
make sure that the newly-minted disclosure authority is not being abused.

The Administration offered three reasons for reneging on the original deal. First, they claimed that the involvement of the court would inhibit Federal investigators and attorneys from disclosing information needed by intelligence and national security officials. Second, they said the courts might not have adequate security and therefore should not be told that information gathered for intelligence or national security purposes. And third, they said the President’s constitutional powers under Article II give him authority to get whatever foreign intelligence he needs to exercise his national security responsibilities.

I believe these concerns are unfounded. Federal investigators and attorneys will recognize the need to disclose information relevant to terrorism investigations. Courts can be trusted to keep secrets and recognize the needs of the presidency.

Current law requires that such information be used only for law enforcement purposes. This provides an assurance that highly intrusive invasions of privacy are confined to the purpose for which they are approved by a court, based on probable cause, as required by the Fourth Amendment. Current law calls for minimization procedures to ensure that the surveillance does not gather information about private conversations that are not relevant to the criminal investigation.

When the Administration reneged on the agreement regarding court supervision, we turned to other safeguards and were more successful in changing other questionable features of the Administration’s bill. The Administration accepted my proposal to strike the term “national security” from the description of wiretap information that may be disclosed throughout the executive branch and replace it with “foreign intelligence” information. This change is important in clarifying what information may be disclosed because the term “foreign intelligence” is specifically defined by statute whereas “national security” is not.

Moreover, the rubric of “national security” has been used to justify some particularly unsavory activities by the government in the past. We must have at least some evidence that we are not embarked on a course that will lead to a repetition of these abuses because the statute will now more clearly define what type of information is subject to disclosure. In addition, Federal officials who receive the information may use it only as necessary to the conduct of their official duties. Therefore, any disclosure or use outside the conduct of their official duties remains subject to all limitations applicable to their retention and dissemination of information of title 18.

This includes the Privacy Act, the criminal penalties for unauthorized disclosure of electronic surveillance information under chapter 119 of title 18, and the contempt penalties for unauthorized disclosure of grand jury information. In addition, the Attorney General must establish procedures for the handling of information of title 18 where the officers search a premises and receive the information. The Administration must be careful not to abuse this authority.

Another issue that has caused me serious concern relates to the Administration’s proposal for so-called “sneak and peek” search warrants. The House Judiciary Committee dropped this proposal entirely from its version of the legislation. Normally, when law enforcement officers execute a search warrant, they must leave a copy of the warrant and a receipt for all property seized at the premises searched. Thus, if the owner of the premises is present, the owner will receive notice that the premises have been lawfully searched pursuant to a warrant rather than, for example, burglarized.

Two circuit courts of appeal, the Second and the Ninth Circuits, have recognized a limited exception to this requirement. When specifically authorized by the issuing judge or magistrate, the officers may delay providing notice of the search to avoid disrupting an ongoing investigation or for some other good reason. However, this authority has been carefully circumscribed.

First, the Second and Ninth Circuit courts of appeal have dealt only with situations where the officers search a premises without seizing any tangible property. As the Second Circuit explained, such searches are “less intrusive than a conventional search with physical seizure because the latter deprives the owner normally of the peaceful use of his property.” United States v. Villegas, 899 F.2d 1324, 899 F.2d 1324, 1337 (2d Cir. 1990).
Second, the cases have required that the officers seeking the warrant must show good reason for the delay. Finally, while the courts have allowed notice of the search may be delayed, it must be provided within a reasonable period thereafter, which should generally be no more than seven days. The reasons for these careful limitations were spelled out succinctly by Judge Sneed of the Ninth Circuit: “The mere thought of strangers walking through and into your home, seeing the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.” United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

The Administration’s original proposal would have ignored some of the key limitations created by the caselaw for sneak and peek warrants. First, it would have broadly authorized officers not only to conduct surreptitious searches, but also to secretly seize any type of property without any additional notice of necessity created by the caselaw. Second, the provision now requires that notice be given a blanket authorization for up to 90 days, instead of the presumptive seven-day period to a maximum of 90 days, the same duration as for United States persons. Experience indicates, however, that after the initial period has confirmed probable cause that the foreign national meets the statutory standard, court orders are renewed repeatedly and the 90-day renewal becomes an unnecessary procedural for investigators taxed with far more pressing duties.

The Administration proposed that the period of electronic surveillance be changed from 90 days to one year in these cases. This proposal did not ensure adequate review after the initial stage to ensure that the probable cause determination is justified over time. Therefore, the bill changes the initial period of the surveillance to 120 days and changes the period for extensions from 90 days to one year. The initial 120-day period provides for a review of the results of the surveillance or search directed at an individual before one-year extensions are requested. These changes do not affect surveillance of a United States person.

The bill also changes the period for physical search under FISA from 45 to 90 days. This change applies to United States persons as well as foreign nationals. Experience since physical search authority was added to FISA in 1994 indicates that 45 days is frequently not long enough to plan and carry out a covert physical search. There is no change in the restrictions which provide that United States persons may not be the targets of search or surveillance under FISA. Rather, the statute finds probable cause to believe that they are agents of foreign powers who engage in specified international terrorist, sabotage, or clandestine intelligence activities that may involve a violation of the criminal statutes of the United States. FISA judges. The bill in section 206, seeks to ensure that the special court established under FISA has sufficient judges to handle the workload. While changing the duration of orders and extensions will reduce the number of cases in some categories, the bill retains the court’s role in pen register and trap and trace cases and expands the court’s responsibility for issuing orders for records and other tangible items needed for counterintelligence and counter terrorism investigations. Upon reviewing the court’s requirements, the Administration requested an increase in the number of federal district judges designated for the court from seven to 11 of whom no less than 3 shall reside within 20 miles of the District of Columbia. The latter provision ensures that more than one judge is available to handle cases on short notice and reduces the need to invoke the alternative of Attorney General approval under the emergency authorities in FISA.

Agent of a foreign power standard. Other changes in FISA and related national security laws are more controversial. In several areas, the bill reflects a serious effort to accommodate the requests for expanded surveillance authority with the need for safeguards against misuse, especially the gathering of intelligence about the lawful political or commercial activities of Americans. One of the most difficult issues was whether to eliminate the existing statutory “agent of foreign power” standards for surveillance and investigative techniques that raise important privacy concerns, but not at the level that the supreme Court has held to require a court order and a probable cause finding under the Fourth Amendment. These include pen register and trap and trace devices, access to business records and other tangible items held by third parties, and access to records that have statutory protection. The intelligence community’s demand for “agent of a foreign power” engaged in international terrorism or clandestine intelligence activities.

However, the “agent of a foreign power” standard in existing laws was designed to ensure that the FBI and other intelligence agencies do not use these surveillance and investigative methods to investigate the lawful activities of Americans in the name of an undefined authority to collect foreign intelligence or counterintelligence information. The FBI’s experience under existing laws since they were enacted at various time over the past 15 years has been that, in practice, the requirement to show reasonable suspicion that a person is an “agent of a foreign power” was rarely met and that the requirement to show probable cause for such activity was almost as burdensome as the standard under comparable criminal law enforcement procedures which require only a showing of reasonable suspicion that a person is an “agent of a foreign power.” The FBI’s experience under existing laws since they were enacted at various time over the past 15 years has been that, in practice, the requirement to show reasonable suspicion that a person is an “agent of a foreign power” was rarely met and that the requirement to show probable cause for such activity was almost as burdensome as the standard under comparable criminal law enforcement procedures which require only a showing of reasonable suspicion that a person is an “agent of a foreign power.”

The FBI’s experience under existing laws since they were enacted at various time over the past 15 years has been that, in practice, the requirement to show reasonable suspicion that a person is an “agent of a foreign power” was rarely met and that the requirement to show probable cause for such activity was almost as burdensome as the standard under comparable criminal law enforcement procedures which require only a showing of reasonable suspicion that a person is an “agent of a foreign power.”
The challenge, then, was to define those investigations. The alternative proposed by the Administration was to cover any investigation to obtain foreign intelligence information. This was extremely broad, because the definition of ‘intelligence information’ with respect to a foreign power that relates to, and if concerning a United States person is necessary to, the national defense or the security of the United States or the conduct of the foreign affairs of the United States. This goes beyond FBI counterintelligence and counterterrorism requirements. Instead, the bill requires that use of the surveillance technique or access to the records concerning a United States person be relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

In addition, an investigation of a United States person may not be based solely on activities protected by the First Amendment. This framework applies to records and other items under section 215, and credit records under section 506. Lawful political protest by American citizens against the government may not be the basis for FBI counterintelligence and counterterrorism investigations under these provisions.

A separate issue for pen registers and trap and trace under section 215, access to records and other items under section 215, and the national security authorities for access to telephone, bank, and credit records under section 506. The Administration initially proposed that the Attorney General ‘may not be the basis for FBI counterintelligence and counterterrorism investigations under these provisions. The Justice Department opinion cites relevant legislative history from the Senate Intelligence Committee’s report in 1978, and there is comparable language in the House report. The Justice Department’s opinion cites relevant legislative history from the Senate Intelligence Committee’s report in 1978, and there is comparable language in the House report.

Immigration. The Administration initially proposed that the Attorney General be authorized to detain any alien indefinitely upon certification of suspicion to links to terrorist activities or organizations. Under close questioning by both Senator KENNEDY and Senator SPETZER at the Committee hearing on September 25, the Attorney General said that his proposal was intended only to allow the government to hold an alien suspected of terrorist activity while deportation proceedings were ongoing. In response to a question by Senator SPETZER, the Attorney General said: “Our intention is to be able to detain individuals who are the subject of deportation proceedings on other grounds, to detain them as if they were the subject of deportation proceedings on terrorism.” The Justice Department, however, continued to insist on broader authority, including some of the power of the alien was found not to be deportable.

I remain concerned about the provision, in section 412, but I believe that it has been improved from the original proposal offered by the Administration. First, the Justice Department must now charge an alien with an immigration or criminal violation within seven days of taking custody, and the Attorney General’s certification of an alien under this section is subject to judicial review. Second, if an alien is found not to be deportable, the Attorney General can only delegate the power to certify an alien to the Deputy Attorney General, ensuring greater accountability and preventing the certification decision from being made by low-level officials. Despite these improvements, I would have preferred that this provision be included, and I would urge the Attorney General and his successors to employ that discretion in using this new power.

In addition, the Administration initially proposed a sweeping definition of terrorist activity and new powers for the Secretary of State to designate an organization as a terrorist organization for purposes of immigration law. We were able to work with the Administration to refine this definition to limit its application to individuals who had innocent contacts with non-designated organizations. We also limited the retroactive effect of these new definitions. If an alien solicited funds or membership, or provided material support for an organization that was not designated at that time by the Secretary of State, the alien would have the opportunity to show that he did not know and should have known that his acts would further the organization’s terrorist activity. This is substantially better than the administration’s proposal, which, in its terms, would have encouraged the INS to target someone who raised money for the African National Congress in the 1980s.

Trade Sanctions. I was disappointed that the Administration’s initial proposal authorizing the President to impose unilateral food and medical sanctions would have undermined a law we passed last year with overwhelming bipartisan support. Under that law, the President already has full authority to impose unilateral food and medicine sanctions during this crisis because of two exceptions built into the law that apply to our current situation. Nevertheless, the Administration sought to undo this law and obtain virtually unlimited authority in the future to impose food and medicine embargoes, without making any effort for a multi-lateral approach in cooperation with other nations. Absent such a multi-lateral approach, other nations feel to step in immediately and take over business from American firms and farmers that they are unilaterally barred from pursuing.

Over 30 farm and export groups, including the American Farm Bureau Federation, the Grocery Manufacturers of America, the National Farmers Union, and the U.S. Dairy Export Council, wrote to me and explained that the Administration proposal was “not achievable its intended policy goal.” I worked with Senator ENZI, and other Senators, on substitute language
to give the Administration the tools it needs in this crisis. This substitute has been carefully crafted to avoid needlessly hurting American farmers in the future, yet it will assure that the U.S. can engage in effective multilateral sanctioning.

This bipartisan agreement limits the authority in the bill to existing laws and executive orders, which give the President full authority regarding this conflict, and grants authority for the President to restrict exports of agricultural products, medicine or medical devices. I continue to agree with then-Senator Ashcroft who argued in 1999 that unilateral U.S. food and medicine sanctions simply do not work when he introduced the “Food and Medicine for the World Act.”

As recently as October 2000, then-Senator Ashcroft pointed out how broad, unilateral embargoes of food or medicine are often counterproductive. Many Republican and Democratic Senators at that time were just last year that the U.S. should work with other countries on food and medical sanctions so that the sanctions will be effective in hurting our enemies, instead of just hurting the U.S. I am glad that with Senator Ashcroft, we were able to make changes in the trade sanctions provision to both protect our farmers and help the President during this crisis.

Money Laundering. Title III of the USA Act consists of a bipartisan bill that was reported out of the Banking Committee on October 4, 2001. I commend the Chairman and Ranking Member of that Committee, Senators Sarbanes and Gramm, for working together to produce a balanced and effective package of measures to combat international money laundering and the financing of terrorism.

I am pleased that the Chairman and Ranking Member of the Banking Committee agreed to the inclusion of the managers’ amendment of a small change to a provision of title III, section 319, relating to forfeiture of funds in United States interbank accounts. As reported by the Banking Committee, this provision included language suggesting that in a criminal case, the government may have authority to seek a pretrial restraining order to prevent exclusion of witnesses or information.

As a result of the acts of heroes, one of whom was former Banking Committee Chairman Senator Thompson, parts of the bill. My efforts have not been completely successful and there are a number of provisions on which the Administration has insisted with which I disagree. Frankly, the agreement of September 30, 2001 would have led to a better balanced bill. I could not support the Administration from renege on the agreement any more than I could have “speeded the process to reconstitute this bill in the aftermath of those breaches. In these times we need to work together to face the challenges of international terrorism. I have sought to do so in good faith.

Mr. President, I reserve the remainder of my time and yield the floor.

The PRESIDING OFFICER. Who yields time?

Mr. HATCH. Mr. President, I enjoyed the remarks of my distinguished colleague from Vermont. I compliment him for the work he has done on this bill and for the hard work, over the last 3 weeks, that he and his staff have put into this bill, as well as other members of the Judiciary Committee as a whole, and, of course, people on my side as well.

Mr. President, I do not intend to take very long, because our colleagues are tired, and I know they would like to go home. I also know that we have a distinguished colleague in the Chamber who has some amendments on which we may have to vote.

Four weeks ago we were a relatively tranquil nation, but on September 11, in what amounted to a astardly attack, an unprovoked attack of war, the World Trade Center was destroyed, along with almost 6,000 people, or maybe more. Our Pentagon was struck by a volitionary act of terrorism.

As a result of the acts of heroes, one of the planes was downed in Pennsylvanía, killing all aboard, including those heroes who made sure that that plane did not strike either the Capitol or the White House. I want to pay special tribute to those people who were so heroic as to give up their own lives to protect the lives of so many others.

There have been so many acts of her- oism and self-sacrifice—the firefighters who gave their lives, the firefighters who worked day and night, and the volunteers who have gone in there, and the mayor of New York City, the Governor and so many others who deserve mention.

This bill, hopefully, will help to at least rectify and redeem some of the problems, problems that have existed ever since September 11.

We did not seek this war; it was thrust upon us. It was an unprovoked attack by people who claim that they represent a religious point of view. In fact, they represent a complete distortion of the religion of Islam. Islamic people do not believe in mur- der, murdering innocent civilians. The Koran does not teach that. They do not believe in suicide. The Koran does not teach that.

This is not a war against Islam; this is a war against terrorism and people who have so little regard for human life that they would do something against innocent civilians that was unthinkable before September 11.

Therefore, we live in a dangerous and difficult world today. It is a different world. And we are going to have to wake up and do the things we have to do to protect our citizenry and, of course, to protect the rest of the world to the extent this great Nation can, with the help of other nations, a number of which have become supportive of our efforts. We are very grateful to them.

But a lot of people do not realize we have terror cells in this country—that has been in the media even—and there are people in this country who are dedicated to the overthrow of America. There are people who are dedicated to terrorism right here within our Nation. And some of these people who have participated in this matter may very well be people who were rightfully in our Nation—or at least we thought we were rightfully in our Nation.

The responsibility of redeeming and rectifying this situation is the responsibility of the Congress, the Justice De- partment, the FBI, the INS, and the Border Patrol. It is our job to provide the tools, and for them to first identify and then eradicate terrorist activity within our borders. And our President has taken the extraordinary step of saying that we are going to go after terri- orists worldwide and those who harbor them.

I agree with the President. I think it is time to do it. It is time to hit them where it hurts. It is time to let them know we are not going to put up with this type of activity.

A few weeks ago, the Justice Depart- ment sent up its legislative proposal. It
was a good legislative proposal. They had a lot of ideas in there that literally we have been trying to get through for years. When we passed the 1996 antiterrorism, effective death penalty act, a number of us tried to get some of these reforms in that time, but we were unsuccessful for a variety of reasons, some very sincere.

The fact is, a lot of the provisions we have in the bill are not brand new; a lot of them have been requested for years. And it has been in play, and we have worked day and night to come up with this particular bill.

I congratulate my partner and my colleague, Senator LEAHY, for his hard work, and his staff's for the work they have done on this bill, and, of course, my own staffers, and, of course, those others I have named.

This has been a very difficult bill to put forward because there are all kinds of cross-pressures, all kinds of ideas, all kinds of different thoughts, all kinds of differing philosophies. We believe, with all kinds of deliberation and work, we have been able to put together a bill that is really making sense, that will give the Justice Department the tools it needs to be able to work and stamp out terrorist activity within our country. At least we want to give them the very best tools we possibly can.

We have tried to accommodate the concerns of Senators on both sides of the aisle. We have worked very hard to do so. We cannot accommodate everybody's concerns. As Senator LEAHY has said, this is not a perfect bill. Nothing ever seems to be perfect around here. But this is as good a bill as can be put together, in a bipartisan way, in this area in the history of the Senate, I really feel good about it, that we have done this type of a job.

As I say, a lot of these provisions have been requested by the Justice Department and both Democrat and Republican White Houses for years. We took into consideration civil liberties, throughout our discussions on this bill. I think we got it just right. We are protective of civil liberties while at the same time giving the tools to the law enforcement agencies to be able to do their jobs in this country.

I might mention that this bill encourages information sharing, that would be absolutely prohibited under current law, among various agencies of Government, information sharing that should have been allowed a long time ago, at least in my view.

It updates the laws with regard to electronic surveillance and brings those laws into the digital age, and brings them into an effective way so that we can, in a modernized way, protect our society, at least to the extent we can, from these types of terrorist activities.

Of course, little things, such as pen registers, trap-and-trace authority—we have been able to resolve these problems after years of problems.

I would like to make a few comments regarding the process for this legislation. Although we have considered this in a more expedited manner than other legislation, my colleagues can be assured that this bill has received thorough consideration. First, the fact is that the bulk of these proposals have been requested by the Department of Justice for years, and have languished in Congress for years because we have been unable to muster the collective political will to enact them into law.

No one can say whether these tools could have stopped the attacks of September 11. But, as the Attorney General has said, it is certain that without these tools, we did not stop the vicious acts of last month. I say to my colleagues, Mr. President, that if these tools could help us now to track down the perpetrators of these monstrous acts and they are, it is difficult to see why anyone would oppose their passage.

Furthermore, I would like to clearly dispel the myth that the reforms in this legislation somehow abridge the Constitutional freedoms enjoyed by law-abiding American citizens. Some press reports have portrayed this issue as a choice between individual liberties on the one hand, and on the other hand, enhanced powers for our law enforcement agencies. This is an unfortunate dichotomy. We should all take comfort that the reforms in this bill are primarily directed at allowing law enforcement agents to work smarter and more efficiently—in no case do they curtail the precious civil liberties protected by our Constitution. I want to assure my colleagues that we worked very hard over the past several weeks to ensure that this legislation upholds all of the constitutional freedoms our citizens cherish.

Mr. President, I will submit for the RECORD my extended remarks describing this legislation, but I would like to take a minute to explain briefly a few of the most important provisions of this critical legislation.

First, the legislation encourages information-sharing between various arms of the federal government. I believe most of our citizens would be shocked to learn that, even if certain government agents had prior knowledge of the September 11 attacks, under many circumstances they would have been prohibited by law from sharing that information with the appropriate intelligence or national security authorities.

This legislation makes sure that, in the future, such information flows freely within the Federal government, so that it will be received by those responsible for protecting against terrorist attacks.

By making these reforms, we are rejecting the outdated Cold War paradigm that has prevented cooperation between our intelligence community and our law enforcement agencies. Current law does not adequately allow for such cooperation, artificially hampering our government's ability to identify and prevent acts of terrorism against our citizens.

In this new war, terrorists are a hybrid between domestic criminals and international agents. We must lower the barriers that discourage our law enforcement and intelligence agencies from working together to stop these terrorists. These hybrid criminals call for new, hybrid tools.

Second, this bill updates the laws relating to electronic surveillance. Electronic surveillance, conducted under the supervision of a federal judge, is one of the most powerful tools at the disposal of our law enforcement community. It is simply a disgrace that we have not acted to modernize the laws currently on the books which govern such surveillance, laws that were enacted before the fax machine came into common usage, and well before the advent of cellular telephones, e-mail, and instant messaging. The Department of Justice has asked us for years to update these laws to reflect the new technologies, but there has always been a call to go slow, to seek more information, to order further studies.

This is no hypothetical problem. We now know that e-mail, cellular telephones, and the Internet have been principal tools used by the terrorists to coordinate their activities. We need to pursue all solid investigatory leads that exist right now that our law enforcement agents would be unable to pursue because they must continue to work within these outdated laws. It is high time that we update our laws so that our law enforcement agencies can deal with the world as it is, rather than the world as it existed 20 years ago.

A good example of why we are hand-capping our law enforcement agencies relates to devices called "pen registers." Pen registers may be employed by the FBI, after obtaining a court order, to determine what telephone numbers are being dialed from a particular telephone. These devices are essential investigative tools which allow law enforcement agents to determine who is speaking to whom, within a criminal conspiracy.

The Supreme Court has held, in Smith v. Maryland, that the information obtained by pen register devices is not information that is subject to any constitutional protection. Unlike the content of your telephone conversation
VerDate 13-OCT-2001 00:54 Oct 13, 2001 Jkt 089060 PO 00000 Frm 00029 Fmt 0624 Sfmt 0634 E:\CR\FM\G11OC6.152 pfrm02 PsN: S11PT2

eral courts have already ruled—that Federal judges may grant pen register orders to cover, not just telephones, but other more modern modes of communication such as e-mail or instant messaging. Let me make clear that the bill does not allow law enforcement to receive the content of the communication, but they can receive the addressing information to identify the computer or computers a suspect is using to further his criminal activity. Importantly, the reform of the pen register order does not allow—as has sometimes been misreported in the press—for law enforcement agents to view the content of any e-mail messages—not even the subject line of e-mails. In addition, this legislation we are considering does not explicitly state that content can not be collected through such pen register orders.

This legislation also allows judges to enter pen register orders with nationwide scope. Nationwide jurisdiction for pen register orders makes common sense. It helps law enforcement agents efficiently identify communications facilities throughout the country, which greatly enhances the ability of law enforcement to identify quickly other members of a criminal organization, such as a terrorist cell.

Moreover, this legislation provides our intelligence community with the same authority to use pen register devices, under the auspices of the Foreign Intelligence Surveillance Act, as for wiretapping. Law enforcement agencies have when investigating criminal offenses. It simply makes sense to provide law enforcement with the same tools to catch terrorists that they already possess in connection with other criminal investigations, such as drug crimes or illegal gambling.

In addition to the pen register statute, this legislation updates other aspects of our wiretapping statutes. It is amazing that law enforcement agencies do not currently have authority to seek wiretapping authority from a Federal judge when investigating a terrorist offense. This legislation fixes that problem.

Moving on, I note that much has been made of the complex immigration provisions of this bill. I know Senators SPECTER, KOHL and KENNEDY had questions about earlier provisions, particularly the detention provision for suspected alien terrorists. I want to assure my colleagues that we have worked hard to address your concerns, and the concerns of the public. As with the other immigration provisions of this bill, we have made painstaking efforts to achieve this workable compromise.

Let me address some of the specific concerns. In response to the concern that the INS might detain a suspected terrorist for 72 hours, the Senator KENNEDY, Senator SPECTER, and I worked out a compromise that limits the provision. It provides that the alien must be charged with an immigration or criminal violation within seven days after the start of the investigation or be released. In addition, contrary to what has been alleged, the certification itself is subject to judicial review. The Attorney General’s power to detain a suspected terrorist under this bill is, then, not unfettered.

Moreover, Senator LEAHY and I have also worked diligently to craft necessary language that provides for the deportation of those aliens who are representatives of organizations that endorse terrorist activity, those who use their position to enduce terrorist activity or persuade others to support terrorist activity, or those who provide material support to terrorist organizations. If we are to fight terrorism, we can not allow those who support terror to remain in our country. Also, I should note that we have worked hard to provide the State Department and the INS the tools they need to ensure that no applicant for admission who is a terrorist is able to secure entry into the United States through legal channels.

Finally, the bill gives law enforcement agencies powerful tools to attack the financial infrastructure of terrorism giving our Government the ability to choke off the financing that these dangerous terrorist organizations need to survive. It criminalizes the practice of harboring terrorists, and puts teeth in the laws against providing material support to terrorists and terrorism organizations. It gives the President expanded authority to freeze the assets of terrorists and terrorist organizations, and provides for the eventual seizure of such assets. These tools are vital to our ability to effectively wage the war against terrorism, and ultimately to win it.

There have been few, if any, times in our nation’s great history where an event has brought home to so many of our citizens, so quickly, and in such a graphic fashion, a sense of our vulnerability to unexpected attack. I believe we all took some comfort when President Bush promised us that our law enforcement institutions would have the tools necessary to protect us from the danger that we are only just beginning to perceive.

The Attorney General has told us what tools he needs. We have taken the time to review the problems with our current laws, and to reflect on their solutions. The time to act is now. Let us please move forward expeditiously, and give those who are in the business of protecting us the tools that they need to do the job.

Mr. President, I think most people understand this is an important bill. All of us understand it needs to be done. All of us understand that these are tools our law enforcement people deserve and need to have. And, frankly, it is just common sense. It makes a real difference with regard to the interdiction of future acts of terrorism in our society.

Nobody can guarantee, when you have people willing to commit suicide in the perpetration of these awful acts, that we will prevent all acts at all times that we can absolutely protect our Nation. But this bill will provide the tools whereby we might be able—and in most cases should be able—to resolve even those types of problems.

So with that, I am happy to yield the floor.

The PRESIDING OFFICER (Mr. DURBIN). Who yields time?
The Senator from Maryland.

Mr. SARBANES. Mr. President, I yield myself 10 minutes.

The PRESIDING OFFICER. The Senator from Maryland is recognized for 10 minutes.

Mr. SARBANES. Mr. President, I rise in very strong support of S. 1510, the Uniting and Strengthening America Act of 2001, and in particular, Title III of S. 1510, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

Title III was passed by the Committee on Banking, Housing, and Urban Affairs, which I am privileged to chair, a week ago today by a unanimous vote of 21 to 0.

President Bush said on September 24: “We have launched a strike on the financial foundation of the global terror network.”

Title III of our comprehensive anti-terrorism package supplies the armament for that strike. Osama bin Laden may have boasted that “al-Qaeda [includes] modern, educated youth who may have boasted that ‘the financial system, as they are aware of the lines in their hands.’” With Title III, we are sealing up those cracks.

Title III contains, among other things, authority to take targeted action against countries, institutions, transactions, or types of accounts the Secretary of the Treasury finds to be of “primary money-laundering concern.” It also contains requirements for due diligence standards directed at corresponding accounts opened at U.S. correspondent foreign banks and banks in jurisdictions that have been found to fall significantly below international anti-money laundering standards.

It contains a bar on the maintenance of U.S. correspondent accounts for offshore shell banks—those banks that have no physical presence or employees anywhere, and that are not part of a regulated and recognized banking company. There is also a requirement that financial institutions establish anti-money laundering programs.

Title III also contains several provisions that should enhance the ability
of the Government to share more specific information with banks, and the ability of banks to share information with one another relating to potential terrorist or money-laundering activities, and a large number of important technical improvements in anti-money laundering laws as well as mandates to the Department of the Treasury to act or formulate recommendations to improve our anti-money laundering programs.

The problem of money laundering is not a new one. There have been significant efforts for some time in Congress to cut the financial lifelines on which criminal operations depend. Senator John Kerry’s exhaustive investigation nearly a decade ago into the collapse of a shady institution called BCCI, which he found was established with “the specific purpose of evading regulation or control by governments,” led him to introduce anti-money laundering legislation. A bill similar to his was approved last year by the Banking Committee of the House of Representatives on a 31 to 1 vote.

Recent investigations by Senator Carl Levin’s Permanent Subcommittee on Investigations produced two reports on the threats large financial institutions face from financial institutions to launder funds and how we can counter these activities. Senator Levin’s report demonstrates dramatically how correspondent banking facilities and private banking services impede financial transparency and hide foreign client identity and activity, thereby contributing to international money laundering.

Senator Charles Grassley has also advocated for stronger money laundering legislation, and sponsored the Money Laundering and Financial Crimes Strategy Act of 1998, which mandates the development of an annual national money laundering strategy.

Two weeks ago we held our own hearings in the Banking Committee. We heard from a number of expert witnesses and from under Secretary of the Treasury Gurule, Assistant Attorney General Chertoff, and Ambassador Stuart Eizenstat, the former deputy secretary of the Treasury.

On October 4, the Banking Committee marked-up and reported out our own bill. The committee print was built on the framework given to us by Senators Kerry, Levin, Grassley, and by others in this institution.

Before describing the provisions of Title III in greater detail, I want to thank all members of the Banking Committee for their contributions to this legislation. As I indicated, it came out of the committee on a vote of 21 to 0. The ranking member, Senator Gramm, provided crucial support. He raised certain issues which were addressed in the approval of the bill.

Senator Enzi has contributed his experience as an accountant in refining another critical provision. Senator Schumer, who has been involved in past efforts to address money laundering activities, played an important role, as did Senators Allard, Bayh, Corzine, and Cramer, who offered amendments and contributed important improvements to various parts of the subtitle.

I am deeply grateful to all of the members of the committee for their strong, positive, and constructive contributions and for their willingness to work day and night. It is my understanding that the committee staff went three consecutive nights without any sleep in order to prepare this legislation. This is carefully considered legislation because it reflects and builds upon efforts which have been made over a number of years.

Earlier today, our colleagues on the Financial Services Committee in the House of Representatives marked-up a bill, many of the provisions of which are identical or virtually identical to those in the Senate bill. Title III of the package now before us.

Public support across the country for anti-money laundering legislation is extremely strong. Jim Hoagland put it plainly in the Washington Post: “This crisis offers Washington an opportunity to force American and international banks to clean up concealment and laundering practices they now tolerate or encourage and which terrorism can exploit.”

Terrorist attacks require major investments of time, planning, training, practice, and financial resources to pay the bills. Money laundering is the transmission belt that gives terrorists the resources to carry out their campaigns of fear. We need to cut off the transmission belt and its ability to bring resources to the networks that enable terrorists to carry out their campaigns of violence.

Title III addresses all aspects of our defenses against money laundering. Those defenses generally fall into three parts. The first is the Bank Secrecy Act, “BSA,” passed in 1970. It requires financial institutions to keep standardized transaction records and report large, unusual or suspicious transactions and mandates reporting of the movement of more than $10,000 in currency into or out of the country. The statute is called the “bank secrecy act,” because it bars banks secrecy in America, by preventing financial institutions from maintaining opaque records, or discarding their records altogether. Secrecy is the hiding place for crime, and Congress has barred our institutions from allowing those hiding places. The bill mandates to bar certain kinds of interbank transactions in which we will not want to participate—banks, broker-dealers, casinos, and non-bank transmitters of funds, currency exchangers, and check cashers—all financial services businesses through which our citizens—and criminals hiding as legitimate citizens—can move funds into and through our economy. Unfortunately, reporting regulations covering some of these institutions have not yet been promulgated.

The second part of our money laundering defenses are the criminal statutes first enacted in 1986 that make it a crime to launder money and allow criminal and civil fines in the redress of crime. The third part is the statutory framework that allows information to be communicated to and between law enforcement officials. Our goal must be to assure—to the greatest extent consistent with reasonable privacy protections—that the necessary information can be used by the right persons in “real time” to cut off terrorism and crime.

Title III modernizes provisions in all three areas to meet today’s threats in our global economy. It has been divided into five subtitles, dealing, respectively, with “international counter-money laundering measures”—sections 311–332—“Bank Secrecy Act improvements”—sections 331–342—bulk cash smuggling—sections 343–344—anti-cash corruption measures—sections 361–363.

There are 30 provisions in Title III. At this time, I want to summarize some of the bill’s most important provisions.

Section 311 gives the Secretary of the Treasury, in consultation with other senior government officials, authority to impose one or more of five new “special measures” against foreign jurisdictions that conceal interbank accounts that the Secretary, after consultation with other senior federal officials, determines to pose a “primary money laundering concern” to the United States. The special measures all involve special recordkeeping and reporting requirements to bar the curtailments behind which launderers hide. In extreme cases the Secretary is permitted to bar certain kinds of interbank accounts from especially problematic jurisdictions. The statute specifies the considerations the Secretary must take into account in using the new authority and contains provisions to supplement the Administrative Procedure Act to assure that any remedies—except certain short-term measures—will be subject to full comment from all affected persons.

This new provision gives the Secretary real authority to act to close overseas loopholes through which U.S. financial institutions are abused. At present the Secretary has no weapons except Treasury Advisories—which don’t impose specific requirements—or full economic sanctions that suspend financial and trade relations with offending targets. President Bush’s invocation of the International Economic Emergency Powers Act (IEEPA) several weeks ago was obviously appropriate. But there are many other situations in which we will not want to
block all transactions, but in which we will want to do more than simply ad-
vising financial institutions about under-
regulated foreign financial institutions or
holes in foreign counter-money
laundering efforts. Former Deputy Sec-
etary Snow testified before the Com-
mittee that adding this tool to the
Secretary’s arsenal was essential.

Section 312 focuses on another aspect
of the fight against money laundering,
the financial institutions that are on
the front lines making the initial dis-
cussions. A large proportion of the
foreign banks that allow inside the United States. It requires
U.S. financial institutions to ex-
crime appropriate due diligence when dealing with private banking accounts
and interbank correspondent rela-
tionships with foreign banks. With respect
to foreign banks, the section requires
U.S. financial institutions to apply ap-
propriate due diligence to all cor-
respondent accounts with foreign
banks, and enhanced due diligence for
accounts of offshore banks or for banks in jurisdictions found to have
substandard money laundering controls
or which the Secretary determines to
be of primary money laundering con-
cern under the new authority given him by Section 311.

The section also specifies certain
minimum standards for the enhanced
due diligence that U.S. financial insti-
tutions are required to apply to ac-
counts opened for two categories of for-
gold—offshore banks and banks in jur-
risdictions with weak anti-money laun-
dering and banking controls. These
minimum standards were developed
from, and are based upon, the factual
record and analysis contained in the
Levin staff report on correspondent
banking and money laundering.

Section 312 is essential to Title III. It
addresses, with appropriate flexibility,
mechanisms whose very importance for the
counter-money laundering efforts makes them special targets of money
launderers, as illustrated in Senator
Levin’s extensive reports and hearings.
A related provision, in section 319, re-
quires foreign banks that maintain cor-
respondent accounts in the United
States to appoint agents for service of
process within the United States and
authorizes the Attorney General and the
Secretary of the Treasury to issue a
summons or subpoena to any such
foreign bank seeking records, wherever
located, relating to any such customer
account or correspondent account. U.S. banks
must sever correspondent arrangements
with foreign banks that do not either com-
ply with or contest any such summons
or subpoena, and if the Attorney Gen-
eral or the Secretary of the Treasury asks them to sever the arrangements.

These provisions send a simple mes-
sage to foreign banks doing business
through U.S. correspondent accounts:
be prepared, if you want to use our
banking facilities, to operate in ac-
cordance with U.S. law.

Section 313 also builds on the factual
record before the Banking Committee
to bar from the United States financial
system pure “brass-plate” shell banks
created outside the U.S. that have no
physical presence anywhere and are
not affiliated with recognized banking
institutions. These shell banks carry
the highest money laundering risks in the
banking world because they are in-
herently unavailable for effective over-
sight—there is no office where a bank
regulator or law enforcement official
can go to observe bank operations, re-
view documents, or make on-site exam-
inations.

Section 317 permits the Secretary
to deal with abuse of another recognized
commercial banking mechanism—con-
centration accounts that are used to
commingle related funds in one place
temporarily pending disbursement or
the transfer of funds into individual
client accounts. Concentration ac-
counts have been used to launder
funds, and the bill permits the Sec-
cretary to issue rules to bar the use of
concentration accounts to move client
funds, as well as documentation linking
funds to their true owners.

Section 312 requires financial insti-
tutions to establish minimum anti-
money laundering programs that in-
clude appropriate policies, procedures,
management, employee training, and
audit features. This is not a “one size
fits all” requirement; in fact its very
generality recognizes that different
types of programs will be appropriate
for different types and sizes of institu-

tions.

A number of improvements are made
to the suspicious activity reporting
rules. First, technical changes strengthen
the safe harbor from civil liability
for institutions that report
suspicious activity to the Treasury.
The provisions not only add to the
protection for reporting institutions; they
also address individual privacy con-
cerns by making it clear that govern-
ment officials are not permitted to
see suspicious transaction reports informa-
tion except in the conduct of their offi-
cial duties. The Act also requires the
issuance of suspicious transaction re-
porting rules applicable to brokers and
dealers in securities within 270 days of
the date of enactment.

Sections 341 and 342 of the Title deal
with underground banking systems such as the Hawala, which is suspected
of being a channel used to finance the
al Qaeda network. Section 341 makes it
clear that underground money trans-
mitters are subject to the same record-
keeping rules—and the same penalties
for violating those rules—as above-
ground, recognized, money trans-
mitters. It also directs the Secretary of
the Treasury to report to Congress,
within one year, on the need for addi-
tional legislation or regulatory con-
trols relating to underground banking
systems. Section 342 authorizes the
Secretary of the Treasury to instruct
the Director of the Federal Reserve or
director of each of the international financial
institutions to use such Director’s
“voice and vote” to support loans and
other use of resources to benefit na-
tions that the President determines to
be contributing to efforts to combat
international terrorism, and to require
the auditing of each international fi-
nancial institution to ensure that
funds are not paid to persons engaged
in terrorism.

Section 351 creates a new Bank Sec-
crecy Act offense involving the bulk
smuggling of more than $10,000 in cur-
rency in any conveyance, article of lag-
gage or merchandise or container, ei-
ther into or out of the United States,
and related forfeiture provisions. This
 provision has been sought for several
years by both the Departments of Jus-
tice and Treasury.

Other provisions of the bill address
relevant provisions of the Criminal Code. These provisions were worked
out with the Judiciary Committee and
are included in Title III because of
their close relationship to the provi-
sions of Title II added or modified by
Title II.

The most important section is 315, which expands the list of specific un-
lawful activities under 18 U.S.C. 1956
and 1957 to include foreign corruption
offenses, certain U.S. export control
violations subject to U.S. ex-
tradition obligations under multilat-
eral treaties, and misuse of funds of
international financial institutions.

Section 316 establishes procedures
to protect the rights of persons whose
property may be subject to confisca-
tion in the exercise of the govern-
ment’s anti-terrorism authority.

Section 319 treats amounts deposited
by foreign banks in interbank accounts
with U.S. banks as having been depos-
ited in the United States for purposes of
the forfeiture rules, but grants the
Attorney General authority, in the in-
terest of fairness and consistent with
the United States’ national interest, to
suspend a forfeiture proceeding based
on a showing that the property is or has
been engaged in or abetted certain
money laundering offenses.

A third important set of provisions
modernize information sharing rules to
reflect the reality of the fight against
money laundering and terrorism.

Section 314 requires the Secretary of
the Treasury to inform financial insti-
tutions, financial regulators and law
enforcement officials and to permit
the sharing of information by law en-
forcement and regulatory authorities
with such institutions regarding per-
sons reasonably suspected, based on
credible evidence, of engaging in ter-
orist acts or money laundering activi-
ties. The section also allows banks to
share information involving possible
money laundering or terrorist activity
among themselves—without notice to the
Secretary of the Treasury.

Section 335 permits, but does not re-
quire, a bank to include information,
in a response to a request for an employment reference by a second bank, about the possible involvement of a former institution-affiliated party in potentially unlawful activity, and creates a safe harbor from civil liability for the bank that includes such information in its employment reference request, except in the case of malicious intent. Given its different focus, it is not my intention to similarly limit a bank's safe harbor from civil liability for the filing of suspicicion activity reports under the Bank Secrecy Act.

Section 340 contains amendments to various provisions of the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, to permit information subject to those statutes to be included in the RECORD. The modernization of our money laundering laws represented by Subtitle III is long overdue. It is not the work of one week or one weekend, but represents a thorough, thoughtful, and dedicated bipartisan effort to produce a piece of prudent legislation. The care taken in producing the legislation extends to several provisions calling for reporting on the legislation's effect and a provision for a three-year review of the legislation's effectiveness.

Subtitle A—INTERNATIONAL COUNTER-MONEY LAUNDERING AND RELATED MEASURES

Sec. 311. Gives the Secretary of the Treasury, in consultation with other senior government officials (in the Secretary's discretion) to impose one or more of five new “special measures” against foreign jurisdictions, entities, transactions and accounts determined after appropriate consultation with other senior federal officials, to determine to pose a “primary money laundering concern” to the United States. The special measures include: (1) requiring identification and recordkeeping or reporting for particular transactions, (2) requiring the identification of the foreign beneficial owners of certain accounts at a financial institution, (3) requiring the identification of customers of a foreign bank who use an interbank payable-through account opened by that foreign bank, (4) after consultation with the Secretary of the Treasury, the Attorney General, and the Chairman of the Federal Reserve Board, to designate, prohibit, or maintain the maintenance of certain interbank correspondent or payable-through accounts. Measures 1-4 may not be imposed, other than by regulation, for a period of one year unless the measures may only be imposed by regulation. Also requires the Secretary of the Treasury, in consultation with the appropriate Federal banking agencies, to keep a record of all measures, within 180 days of the date of enactment, recommendations for the most effective way to require foreign nationals opening a U.S. bank account to comply with the regulations comparable to that required when U.S. citizens open a bank account.

Sec. 312. Requires a U.S. financial institution that maintains a correspondent account or private banking account for a non-United States person to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering. Creates a minimum anti-money laundering due diligence standards for U.S. financial institutions that enter into correspondent banking relationships with banks that operate under offshore banking licenses or under banking licenses issued by countries that do not provide due diligence standards that are cooperative with international counter money laundering principles, or (b) have been the subject of special measures authorized by Sec. 311. Prohibits the Secretary of the Treasury from issuing regulations to encourage cooperation among financial institutions, financial regulators and law enforcement officials and to permit the sharing of information by law enforcement and regulatory authorities with such institutions regarding persons reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. Allows (with notice to the Secretary of the Treasury) the sharing of information among banks involving possible terrorist or money laundering activity.

Sec. 315. Expands the list of specified unlawful activities under 18 U.S.C. 1956 and 1957 to include the possession of money laundering offenses, certain U.S. export control violations, and misuse or use of the IMF.

Sec. 316. Establishes procedures to protect the rights of persons whose property may be subject to confiscation in the exercise of the government's anti-terrorism authority.

Sec. 317. Gives the United States' governments "long-arm" jurisdiction over foreign persons committing money laundering offenses in the United States, over foreign United States bank accounts, and over foreign persons seizing assets ordered forfeited by a U.S. court.

Sec. 318. Expands the definition of financial institution for purposes of 18 U.S.C. 1956 and 1957 to include banks operating outside the United States.

Sec. 319. Treats amounts deposited by foreign banks in interbank accounts with U.S. banks as having been deposited in the United States for purposes of the forfeiture rules, but grants the Attorney General authority, in the interest of justice and consistent with the United States' national interest, to suspend a forfeiture proceeding based on that presumption. Requires U.S. financial institutions to reply to a request for information from a U.S. regulator relating to anti-money laundering matters within 120 hours of receipt of such a request. Requires foreign banks that maintain correspondent accounts in the United States to appoint agents for service of process within the States and authorizes the Attorney General and the Secretary of the Treasury to issue a summons or subpoena to any such foreign bank seeking records, within 30 days of such request, to such a correspondent account. Requires U.S. banks to sever correspondent arrangements with foreign banks that do not either comply with or contest such summons or subpoena. Authorizes United States courts to order a convicted criminal to return property located abroad and to order a civil forfeiture defendant to return property located abroad pending trial on the merits. Authorizes United States prosecutors to use a court-appointed private attorney to represent a criminal defendant's assets, wherever located.

Sec. 320. Permits the United States to institute forfeiture proceedings against the proceeds of foreign criminal offenses committed in the United States.

Sec. 321. Allows the United States to exclude any alien that the Attorney General knows or has reason to believe is or has engaged in or abetted certain money laundering offenses. Extends the prohibition against the maintenance of a forfeiture proceedings on behalf of a fugitive to include a proceeding by a corporation whose majority shareholder is a fugitive and a proceeding in which the corporation's claim is instituted by the fugitive.

Sec. 322. Permits the government to seek a restraining order to preserve the availability of property subject to a foreign forfeiture or confiscation judgment.

Sec. 324. Increases from $100,000 to $1,000,000 the maximum civil and criminal penalties for a violation of provisions added to the Bank Secrecy Act by sections 311 and 312 of the Act.

Sec. 325. Directs the Secretary of the Treasury, in consultation with the Attorney General, the Federal banking agencies, the SEC, the CFTC and other appropriate agencies to evaluate operation of the provisions of Subtitle A of Title III of the Act and recommends to Congress, on or before October 1, 2002, a report containing a recommendation as to whether the provisions should be made permanent, modified or added to the Bank Secrecy Act.

Sec. 326. Directs the Secretary of the Treasury to report annually to the Senate Banking Committee and House Financial Services Committee on measures taken pursuant to Subtitle A of Title III of the Act.

Sec. 327. Authorizes the Secretary of the Treasury to issue regulations concerning the
maintenance of concentration accounts by U.S. depository institutions to prevent an institution’s customers from anonymously directing funds into or through such accounts. Sec. 327. Provides for removal of criminal penalties on officials who violate their trust in connection with the administration of Title III.

SUBTITLE B. CURRENCY TRANSACTION REPORTING AMENDMENTS AND RELATED IMPROVEMENTS

Sec. 331. Clarifies the terms of the safe harbor from civil liability for financial institutions engaging in suspicious activity reports pursuant to 31 U.S.C. 5318(g).

Sec. 332. Requires financial institutions to establish anti-money laundering programs and grants the Secretary of the Treasury authority to set minimum standards for such programs.


Sec. 334. Adds “money laundering related to terrorist funding” to the list of subjects to be dealt with in the annual National Money Laundering Strategy prepared by the Secretary of the Treasury pursuant to the “Money Laundering and Financial Crimes Strategy Act of 1998.”

Sec. 335. Permits (but does not require) a bank to include information, in a response to a request for an employment reference by a second bank, about the possible involvement of a former institution-affiliated party in potentially unlawful activity, and creates a safe harbor from civil liability for the bank that includes such information in response to an employment reference request, except in the case of malicious intent.

Sec. 336. Requires the Bank Secrecy Act Advisory Group to include a privacy advocate among its membership and to operate under certain of the “sunshine” provisions of the Federal Advisory Committee Act.

Sec. 337. Directs the Secretary of the Treasury and the Federal bank regulatory agencies to submit reports to Congress, one year after the date of enactment, containing recommendations for possible legislation to conform the penalties imposed on depository institutions for violations of the Bank Secrecy Act with penalties imposed on such institutions under section 8 of the Federal Deposit Insurance Act.

Sec. 338. Directs the Secretary of the Treasury, after consultation with the Securities and Exchange Commission and the Federal Reserve Board, to promulgate regulations, within 270 days of the date of enactment, requiring broker-dealers to file suspicious activity reports. Also requires the Secretary of the Treasury, the SEC, Federal Reserve Board, and the CFTC to submit jointly to Congress, within one year of the date of enactment, recommendations for effective application of the provisions of 31 U.S.C. 5311–30 to both registered and unregistered investment companies.

Sec. 339. Contains amendments to various provisions of the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, to permit information to be used in the conduct of United States intelligence or counterintelligence activities to prevent international terrorism. Sec. 341. Clarifies that the Bank Secrecy Act treats certain underground banking systems as financial institutions, and that the administrative procedures applicable to licensed money transmitters also apply to such underground systems. Directs the Secretary of the Treasury to report to Congress, within one year of enactment, on the need for additional legislation or regulatory controls relating to underground banking systems.

Sec. 342. Authorizes the Secretary of the Treasury to instruct the United States Executive Director of each of the international financial institutions (for example, the IMF and the World Bank) to use such Director’s “voice and vote” to support loans and other use of resources to benefit nations that the President determines to be contributing to international terrorism, and to require the auditing of each international financial institution to ensure that funds are not paid to persons engaged in terrorism.

SUBTITLE C. CURRENCY CRIMES

Sec. 351. Creates a new Bank Secrecy Act offense involving the bulk smuggling of more than $10,000 in currency in any conveyance, article of liquidation or container, either into or out of the United States, and related forfeiture provisions.

SUBTITLE D. ANTI-CORRUPTION MEASURES

Sec. 361. Expresses the sense of Congress that the United States should take all steps necessary to identify the proceeds of foreign government corruption that have been deposited in United States financial institutions and return such proceeds to the citizens of the country to whom such assets belong.

Sec. 362. Expresses the sense of Congress that the United States must continue actively and publicly to support the objectives of the 29-country Financial Action Task Force Against Money Laundering.

Sec. 363. Expresses the sense of Congress that the United States, in its deliberations and negotiations with other countries, should promote international efforts to identify and prevent the flow of funds to and from terrorist organizations.

SUBTITLE E. MISCELLANEOUS

Sec. 371. Expands the SEC’s emergency order authority.

Sec. 372. Creates uniform protection standards for Federal Reserve facilities.

Mr. LEAHY. Mr. President, I thank the distinguished chairman of the Banking Committee, the senior Senator from Maryland, Mr. SARBANES. He did unbelievable work in this committee, with a committee that was very, very concerned about anti-money laundering—a very complex and difficult subject. He did it unanimously, I believe, in a committee that probably has as diverse a membership—that is an understatement—as one might find. I compliment him and thank him for his kind words.

I reserve the remainder of my time. I see the chairman of the Senate Intelligence Committee here, who wishes to give his opening statement.

The PRESIDING OFFICER. The Senator from New York is recognized.

Mr. REID. Mr. President, I conferred with Senator Daschle a few minutes ago. It is his desire—so there is no misunderstanding of the Members—that a number of opening statements be given: The Senator from Florida, the chairman of the Intelligence Committee, and we understand Senator Stabenow wishes to speak, and there may be a couple of other opening statements.

As soon as that is done, we are going to turn to Senator Feingold to offer the first of his amendments. After that, there will be a vote on the first Feingold amendment.

Mr. LEAHY. Mr. President, I yield 10 minutes to the senior Senator from Florida.

The PRESIDING OFFICER. The Senator from Florida is recognized for 10 minutes.

Mr. GRAHAM. Mr. President, I wish to commend Senators Daschle and Lott for their leadership in bringing this critical piece of legislation to the Senate just 1 month after the horrific events of September 11. Senators LEAHY and HATCH also deserve credit for moving quickly to shape thejudiciary components of this bill and choreograph other provisions, including those affecting the intelligence agencies.

My remarks will focus on title IX of this legislation, which is entitled “Improved Intelligence,” as well as the other provisions in the bill that directly affect the mission of the agencies of the intelligence community.

Title IX is derived from S. 1448, legislation which was developed within the intelligence community, entitled “Intelligence to Prevent Terrorism Act of 2001.”

Since long before September 11, I have been working with members of the committee, particularly Senators Feinstein and Kyl, on comprehensive counterterrorism legislation. Most of the provisions of our bill, with some changes requested by the administration, have now become title IX of S. 1510.

The provisions in title IX, as well as other provisions in the bill, are designed to accomplish a daunting but not impossible task. That task is to change the cultures within the Federal law enforcement and intelligence agencies—primarily the FBI and the CIA—so they work seamlessly together for the good of the American people.

Both the FBI and the CIA are very good. They are the standards of the world in their own missions. But those missions are very different, as are the mandates of the Federal Bureau of Investigation is goal oriented. A criminal case has a beginning, a middle, and an end. In a case that has developed the guilty party, the end is a conviction for the crime committed. The information collected during a criminal case is useful. It is held closely because its purpose is to result in the successful prosecution of an event that occurred in the past—not to inform thinking about what may happen now or in the future. The Central Intelligence Agency, on the other hand, as well as its other companions in the intelligence community, has a global approach, literally
and figuratively. The CIA is restricted to activities outside the United States of America. The CIA collects information on a worldwide basis, and it processes that information, analyzes that information, and it places it in the hands of others. Its customers are other Federal agencies and senior policymakers, including the President of the United States. The purpose of that information is to allow those senior policymakers to make more informed decisions.

Given the threats we now face, the cultures growing out of these different missions must be melded. We cannot fight terrorism by putting yellow tape around a bomb site, calling it a crime scene, collecting evidence, and proceeding to trial frequently years later. We must put the evidence collected after such an event to work for us in real time so we can predict and prevent the next attack. If there is a single goal that the national security components of this antiterrorism bill, it is to change the focus from responding to acts that have already occurred to preventing the acts which threaten the lives of American citizens in this country and abroad.

It is critical that all information lawfully available to the Federal Government be used efficiently and effectively to fight terrorism. We cannot continue to use critical information only in a criminal trial. Any information collected must be available to intelligence officials to inform their operational initiatives so as to prevent the next attack.

Along these lines, several provisions of S. 1510 are designed to change the way information is handled within the Federal Government. For example, section 203 permits law enforcement to share information collected in grand jury proceedings and from title III criminal wiretaps with intelligence agencies. Current law, as it has been interpreted, prevents that sharing, except in very limited circumstances.

Section 908 of this bill, known as the Intelligence Community Amendments Act of 1998, has been complemented by section 203 in that it requires law enforcement officers, FBI agents, and the Justice Department prosecutors to provide foreign intelligence derived in the course of a criminal investigation, including grand jury use, wiretaps, FBI interviews, and the like, to the Central Intelligence Agency and to other intelligence agencies. A “permissive” approach is not good enough under current circumstances. Too many lives have been lost. Too many lives are at risk. Law enforcement sharing of information with the intelligence agencies must be mandatory.

Section 908 further complements this legislation by providing the training of law enforcement officers at the Federal, State, and local agencies so they will be better equipped to recognize foreign intelligence information when they see it, and to get it to the right place on a timely basis.

Let me give a couple of hypothetical but eerily-close-to-reality examples. It is likely that there are, tonight, grand juries meeting at various places in the United States to deal with issues related to the events of September 11. Witnesses may be providing information—information about training camps in Afghanistan, ground warfare techniques used by the Taliban, the types and quantity of weapons available. This type of information will be critical for the military—critical for the military now, not 2 years from now when these cases might go to trial.

Another example is in the area of wiretaps. Let me just take two wiretaps. One has been issued under the Foreign Intelligence Surveillance Act because there was a finding by a Federal judge that there was credible evidence that the telephone was being used by an agent of a foreign power.

In the course of listening to the wiretap, this conversation comes across: I am planning to fly from a specifically designed training camp in Central America to a city in Texas. I am going to take my flight a week from Monday. My intention is, once I arrive over that city, to distribute chemical or biological materials that will terrorize the people of that city in a manner that will cause the illmenses that will be provoked.

But how are you going to pay for this? You don’t have the money to buy a plane, chemicals, or get the expertise necessary to do that? I am going to rob a bank next Monday in order to get the money that I need to pay for this operation. The bank is going to be located at the corner of First and Main, and I am going to do it 3 hours after the bank closes next Monday.

The person listening to that conversation with a foreign intelligence wiretap is under a legal obligation to make known to the appropriate law enforcement officials about a bank robbery at a specific location on a specific date and time in a certain Texas city.

Conversely, if that exact conversation had taken place under a criminal wiretap under title 3, the person listening to that conversation would be prohibited from telling the foreign intelligence agencies that there was about to be a terrorist attack on a date certain against a specific Texas city originating at a specific site in Central America.

Try to convince the American people that makes sense. It clearly does not in today’s reality. This legislation is going to make the same requirement of mandatory sharing when the information is gathered under a criminal wiretap that involves foreign intelligence information, as is the case today when information gathered under a Foreign Intelligence Surveillance Act wiretap must be made available to appropriate law enforcement officials.

Another provision of title 9 addresses the role of the Director of Central Intelligence in the process of collecting foreign intelligence under the Foreign Intelligence Surveillance Act. It recognizes the need to target limited resources, including personnel and translators against the highest priority targets.

I ask if I can have an additional 5 minutes.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. I have about 11 minutes left that has not been committed which I thought I might use to answer some questions. I give the Senator 2 of my 11 minutes.

Mr. GRAHAM. I appreciate the Senator’s limitations.

Mr. LEAHY. We just had one Senator ask me for 30 minutes. I am looking at my 11. How can I give him 30? But I will give you 2 of the 11.

Mr. GRAHAM. Mr. President, I thank the Senator from Vermont.

We have a provision that the Director of Central Intelligence, the DCI, will set the overall strategic goals for the collection of foreign intelligence so that we can use our limited resources as effectively as possible.

In order to complement that, we also have a provision that will establish a national virtual translation center as a means of increasing our woefully limited linguistic capabilities to translate the material which we are gathering.

We will also provide for additional capability with human intelligence. We have one of the best-performing technologies—eavesdropping, satellite imagery, to the exclusion of the use of human beings. If we want to gain information about the bin Ladens of the world, we cannot just take a picture of bin Laden.

Today it is increasingly difficult to eavesdrop on bin Laden. What we need to do is get a human being who is able to get close enough to bin Laden to learn his intentions and capabilities. This gets to the difficult issue of what kind of assets, human beings, we hire to work for us to gather such information?

We would all like to employ the purist of people, all choir boys to do this type of work. Unfortunately, they are not the type of people who are likely to be able to get close to the bin Ladens of the world. Thus, we have a provision in this legislation in the nature of a sense of Congress which we hope will send a very strong message to the intelligence community that we are encouraging them to overcome some previous messages from Congress and to proceed to recruit the persons who they find to be necessary to gain access to terrorists so that we can have the best opportunity of protecting our nation.

With the adoption of this legislation, we have not reached the end of our task or responsibilities to protect the American people. We are taking a substantial step in that direction.

To reiterate, another provision of title 9 addresses the role of the Director of Central Intelligence in the process of collecting foreign intelligence.
under the Foreign Intelligence Surveillance Act. It recognizes the need to target limited resources—e.g., translators—against the highest priority targets.

In order to ensure that scarce resources are effectively used, the DCI—in his role as head of the Intelligence Community, not as CIA Director—will set overall strategic goals for FISA collection.

He will work with the Attorney General to ensure that FISA information is distributed to the intelligence operators and analysts who need it government-wide.

Of course, the operational targeting and collection using wiretaps will be conducted by the FBI, as it has in the past; the DCI will perform no role in those decisions.

One of the scarce resources that has plagued the Intelligence Community, as well as law enforcement, is translation capability.

Section 907 of this bill requires the FBI and CIA to work together to create a “National Virtual Translation Center.”

Such a center would seek to remedy the chronic problem of developing critical language abilities, and matching those resources to intelligence collected by the wide range of techniques available.

It is not enough to be able to listen to the conversations of terrorists and their supporters. Those conversations must be translated, often from difficult languages such as Urdu, and analyzed, all in a timely fashion.

Our intelligence services collect vast amounts of data every day. It is possible that we may find that a critical clue to the September 11 attacks may have been available, but untranslated, days, weeks, or even months before the hijackings.

We must address this problem before another specific threat is overlooked.

Finally, I would like to mention a problem that has received a great deal of attention in recent weeks. There has been criticism of the intelligence agencies for placing too great a reliance on technical intelligence collection—lawns dropping, satellite photograph—in recent years at the expense of human sources, or spies.

A corollary of this criticism is that CIA officers are too risk-averse and that they do not aggressively recruit sources, including those that may have access to terrorist groups because the sources may have engaged in human rights violations or violent crimes.

As to the first problem, the Intelligence Authorization bill for fiscal year 2002, which may come to the floor next week, provides greater resources for human source recruitment—and it is part of a 5-year plan to beef up this method of collection.

With respect to the second problem, we in this Congress simply must accept some of the responsibility for creating a risk-averse reaction at CIA, if needed there is one.

The internal CIA regulations addressing the so-called “dirty asset” problem grew out of the criticisms by Congress in the mid-1990s about the recruitment of sources in Guatemala with sordid pasts.

We address this issue in S. 1510, section 903, by sending a strong message to CIA Headquarters and CIA officers overseas that recruitment of any person who has access to terrorists or terrorist groups should be of the highest priority.

There is no place in times like these for timidity in seeking every method available to learn the capabilities, plans, and intentions of terrorists.

Congress needs to send a strong message that we value such efforts to recruit sources on terrorism, even those with pasts we would not applaud. Section 903 sends that message. I urge passage of S. 1510.

I again commend the Members of the Senate who have played such an effective role.

I also thank the staff: Al Cumming, Vicki Divoll, Steven Cash, Bill Duhnke, Paula DeSutter, Jim Hensler, and Jim Barnett.

They have been working for the past many months to bring us to the point of this legislation being available for adoption by the Senate tonight and for the safety of the American people.

The PRESIDING OFFICER. The time of the Senator has expired. The Senator from Vermont.

Mr. LEAHY. I ask the distinguished Senator from Utah—I see the distinguished senior Senator from Pennsylvania is here—perhaps after the senior Senator from Utah, and then after the senior Senator from Pennsylvania speaks, whether it might be possible to go to the Senator from Wisconsin for the purpose of bringing up his amendments, and we can then debate and vote on them. Will that be agreeable to everybody?

Mr. HATCH. It is agreeable.

Mr. LEAHY. I ask unanimous consent that after the Senator from Utah, and the Senator from Pennsylvania, we go to the Senator from Wisconsin for the purpose of bringing up his amendments.

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

The Senator from Utah.

Mr. HATCH. Mr. President, in my opening remarks, I was remiss in not mentioning the tremendous work of the distinguished chairman and vice chairman of the Intelligence Committee. They have done a tremendous amount of work on the intelligence aspect of this bill. As a member of the Intelligence Committee, I express my high regard for the both of them and the work they have done.

I also express my regard for my friend from Maryland, Senator Sar-\n\nThe PRESIDING OFFICER. The Senator from Pennsylvania.

Mr. SPECTER. Mr. President, I have sought recognition and asked for this reservation of time to express my concerns about the record which the Senate is creating so that whatever legislation we pass will pass constitutional muster.

The Supreme Court of the United States has handed down a series of decisions in the past decade which question the constitutionality and, in fact, invalidate acts of Congress because there has been an insufficient record compiled. So I make these statements and review the record so far with a view to urging my colleagues to create a record in this Chamber, in conference, or wherever that opportunity may present itself.

In 1989, in the case of Sable v. FCC, the Supreme Court of the United States struck down an act of Congress saying, “no Congressman or Senator purported to present a considered judgment.” I thought it was a remarkable statement by the Supreme Court since Congressman Tom Billey in the House of Representatives had established a very comprehensive record.

The Supreme Court in 1997, in a case captioned Reno v. ACLU, again invalidated an act of Congress noting, “the lack of legislative attention to the statute at issue in Sable suggests another parallel with this case.”

It was surprising to me that the Supreme Court of the United States would invalidate an act of Congress on the ground that no Senator or Congressman had purported to present a considered judgment, when that is the view of the Supreme Court which is contrary to Congress.

Under our doctrine of separation of powers, it seemed to me an act of Congress should stand unless there is some specific provision in the Constitution which warrants invalidating it or for vagueness under the due process clause of the Fifth Amendment.

The Supreme Court of the United States, in January of last year, did it again in a case captioned Kimel v. Florida Board of Regents, a case which involved the Age Discrimination in Employment Act. There the Court said, “our examination of the act’s legislative record confirms that Congress’ 1974 extension of the Act to the States
was an unwarranted response to a perhaps inconsequential problem." Again, a remarkable holding that the Congress had an unwarranted response and that it was an inconsequential problem, totally contradicting the judgment of the Congress of the United States.

Then the Court went on in the Kimel case to say, "Congress had no reason to believe that broad prophylactic legislation was necessary in this field."

The President has raised a few of the cases where the Supreme Court of the United States has invalidated acts of Congress. There is no doubt there is a need for legislation to expand the powers of law enforcement to enable us to act against terrorists. My own experience in 8 years on the Intelligence Committee, 2 years of which was as chairman, and my work as chairman of the Judiciary Subcommittee on Terrorism have convinced me without a doubt of the scourge of terrorism which we have seen many times but never with the intensity which we observed on September 11 of this year.

The act of Congress in expanding law enforcement has to be very carefully calibrated to protect civil liberties and be in accordance with the Constitution of the United States. Attorney General Ashcroft met with a number of us on Wednesday, September 19, just 8 days after the incident of September 11, and asked that we enact legislation by the end of the week. My response at that time was I thought it could not be done in that time frame, but I thought we could hold hearings in the remainder of that week, perhaps on Thursday the 20th, or Friday the 21st, or Saturday the 22nd, to move ahead, understanding the import of the administration's bill, and legislate to give them what they needed, consistent with civil rights.

The Judiciary Committee then held a hearing on September 25 where the Attorney General was summoned for about an hour and 20 minutes. At that time, as that record will show, only a few Senators were able to ask questions. In fact, the questioning ended after my turn came, and most of the Judiciary Committee did not have a chance to raise questions.

On September 26, the following day, I wrote to the chairman of the committee saying:

I write to urge that our Judiciary Committee proceed promptly with the Attorney General's terrorism package with a view to mark up the bill early next week so the full Senate can consider it by the end of the week. I am concerned that some further delay in terrorism may occur which would be attributable to our failure to act promptly.

I then found out on October 3 that the subcommittee on the Constitution was having a hearing. By chance, I heard about it in the corridors. Although I was unable to attend a hearing with the Health and Human Services Secretary Thompson on bioterrorism, I absented myself from the bioterrorism hearing and went down the hall to the Judiciary subcommittee hearing and participated there and expressed many of the reservations and concerns I am commenting about today.

On that date, I again wrote to Senator LEAHY. I asked unanimous consent to submit a letter to him and the full text of his reply to me of October 9 be printed in the RECORD at the conclusion of these remarks.

The PRESIDING OFFICER. Without objection, it is so ordered. (See exhibit 1.)

Mr. SPECTER. I quote only from the first sentence of Senator LEAHY's response to me:

I thank you for your letters of September 26 and October 3 and for your participation in the September 25 hearing regarding antiterrorism legislation. On October 3, you wrote that you were concerned about the lack of hearings. I share that concern and have tried to notice prompt hearings on a number of aspects of the legislative proposals at the earliest possible time.

On this state of the record, which I hope can yet be perfected, I am concerned about our meeting the standards of the Supreme Court of the United States for a sufficient deliberative process.

When Attorney General Ashcroft appeared before the Judiciary Committee on September 25, he said the only detention he wanted on alleged terrorists who were about to be deported proceeded. I then pointed out, as the record will show, that the legislation submitted by the Attorney General was much broader and did not limit detention simply or exclusively to those who were subject to deportation proceedings. So my comment was that it was necessary to analyze the bill very carefully, not do it hurriedly, and give the Attorney General of the Department of Justice what he needed, consistent with constitutional rights.

The other issue which I had an opportunity to raise in the very brief period of time I had—some 5 minutes—involved modifications to the Foreign Intelligence Surveillance Act, where the issue was to change the law from "the purpose," being the gathering of intelligence, to "a purpose." Ultimately the legislation has been modified to read "a significant purpose."

At that hearing, the Attorney General said not long to obtain content from electronic surveillance unless probable cause was established. But in the draft bill, which the Department of Justice had submitted at that time, that was not what the bill provided. So that on this state of the record, I think the Congress has some work to do, tonight in conference or perhaps by other means, to see to it we have a record which will withstand constitutional scrutiny.

On our Judiciary Committee, we have many Members who have expertise in this field. This bill, as the RECORD will show, was negotiated by the chairman and ranking member with the Department of Justice, with the participation of the committee only to the extent of the hearing of the full committee on September 25 and the subcommittee on October 3.

We have on our Judiciary Committee a number of Members who have had experience as prosecuting attorneys. We have a number of Members who are learned in law. We have other Members who have extensive experience on the Judiciary Committee and a great deal of common sense which may top some of us who have prosecutorial experience or extended experience with probable cause and search warrants or surveillance of some sort or another.

I express these concerns so whatever can be done by the Congress will be done to meet the constitutional standards.

How much of the 15 minutes have I used?

The PRESIDING OFFICER. The Senator has 3 minutes 37 seconds remaining.

Mr. SPECTER. I reserve the remainder of my time, and I yield the floor.

EXHIBIT 1


Hon. PATRICK J. LEAHY, Chairman, Senate Judiciary Committee, Wash-

ington, DC.

Dear Mr. SPECTER: I quote only from the first sentence of Senator LEAHY's response to me:

I thank you for your letters of September 26 and October 3 and for your participation in the September 25 hearing regarding antiterrorism legislation. On October 3, you wrote that you were concerned about the lack of hearings. I share that concern and have tried to notice prompt hearings on a number of aspects of the legislative proposals at the earliest possible time.

On this state of the record, which I hope can yet be perfected, I am concerned about our meeting the standards of the Supreme Court of the United States for a sufficient deliberative process.

When Attorney General Ashcroft appeared before the Judiciary Committee on September 25, he said the only detention he wanted on alleged terrorists who were about to be deported proceeded. I then pointed out, as the record will show, that the legislation submitted by the Attorney General was much broader and did not limit detention simply or exclusively to those who were subject to deportation proceedings. So my comment was that it was necessary to analyze the bill very carefully, not do it hurriedly, and give the Attorney General of the Department of Justice what he needed, consistent with constitutional rights.

The other issue which I had an opportunity to raise in the very brief period of time I had—some 5 minutes—involved modifications to the Foreign Intelligence Surveillance Act, where the issue was to change the law from "the purpose," being the gathering of intelligence, to "a purpose." Ultimately the legislation has been modified to read "a significant purpose."

At that hearing, the Attorney General said not long to obtain content from electronic surveillance unless probable cause was established. But in the draft bill, which the Department of Justice had submitted at that time, that was not what the bill provided. So that on this state of the record, I think the Congress has some work to do, tonight in conference or perhaps by other means, to see to it we have a record which will withstand constitutional scrutiny.

On our Judiciary Committee, we have many Members who have expertise in this field. This bill, as the RECORD will show, was negotiated by the chairman and ranking member with the Department of Justice, with the participation of the committee only to the extent of the hearing of the full committee on September 25 and the subcommittee on October 3.

We have on our Judiciary Committee a number of Members who have had experience as prosecuting attorneys. We have a number of Members who are learned in law. We have other Members who have extensive experience on the Judiciary Committee and a great deal of common sense which may top some of us who have prosecutorial experience or extended experience with probable cause and search warrants or surveillance of some sort or another.

I express these concerns so whatever can be done by the Congress will be done to meet the constitutional standards.

How much of the 15 minutes have I used?

The PRESIDING OFFICER. The Senator has 3 minutes 37 seconds remaining.

Mr. SPECTER. I reserve the remainder of my time, and I yield the floor.

Sincerely,

ARLEN SPECTER.


Hon. PATRICK J. LEAHY, Chairman, Senate Judiciary Committee, Wash-

ington, DC.

Dear Mr. SPECTER: I am very much concerned about the delay in acting on the anti-terrorism legislation and also about the absence of hearings to establish a record for the legislative package.

In recent decisions, the Supreme Court of the United States has declared acts of Congress unconstitutional when there has been an insufficient record or deliberative process to justify the legislation.

On our Judiciary Committee, we have many Members who have expertise in this field. This bill, as the RECORD will show, was negotiated by the chairman and ranking member with the Department of Justice, with the participation of the committee only to the extent of the hearing of the full committee on September 25 and the subcommittee on October 3.

We have on our Judiciary Committee a number of Members who have had experience as prosecuting attorneys. We have a number of Members who are learned in law. We have other Members who have extensive experience on the Judiciary Committee and a great deal of common sense which may top some of us who have prosecutorial experience or extended experience with probable cause and search warrants or surveillance of some sort or another.

I express these concerns so whatever can be done by the Congress will be done to meet the constitutional standards.

How much of the 15 minutes have I used?

The PRESIDING OFFICER. The Senator has 3 minutes 37 seconds remaining.

Mr. SPECTER. I reserve the remainder of my time, and I yield the floor.

Sincerely,

ARLEN SPECTER.
Mr. LEAHY. I understand the distinguished Senator from Wisconsin is willing to have the distinguished Senator from Michigan recognize him for a few minutes. I ask unanimous consent she be allowed to proceed preceding the Senator from Wisconsin.

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

Ms. STABENOW. I thank our distinguished chairman and my friend from Wisconsin for allowing me to proceed before he presents his amendments.

I rise this evening to congratulate all involved in this effort. As has been said on so many occasions, it is not perfect but we have come together with a very positive, important step forward that we can control and create this evening on a bipartisan basis.

As the Senator from Michigan, along with my colleague, Senator LEVIN, we certainly celebrate the efforts along the northern border and the important authorizations for dollars that allow us to continue to protect and strengthen the efforts at the border. I thank my chairman of the Banking Committee, Senator SARBANES, for his efforts to put into this important bill language dealing with the critical issue of money laundering which essentially allows us to follow the money.

My colleague, Senator LEVIN, has been extremely involved in helping to lead efforts to lay the case for this. Senator KERRY and Senator GRASSLEY have been in important work. I thank them.

The antiterrorism bill before the Senate takes a significant step forward in cutting off terrorist money. As the President has repeatedly said, stopping the flow of money is key to stopping terrorism. That is what we are doing this evening. In particular, we are establishing important new responsibilities, both for our Government and for our financial institutions. The bill authorizes the Treasury Secretary to take special measures to stop suspected money-laundering activities. This anti-money-laundering language is significant because it requires financial institutions to set up their own due diligence to combat money laundering, particularly for private and corresponding banking situations. This is a key provision of which I was proud to be a part. I am pleased we were able to come up with language that allows that.

Another important provision I was pleased to offer in the Banking Committee, which is now part of the bill, was clear authority for the Treasury Secretary to issue regulations to stop this money laundering which essentially allows us to follow the money. This anti-money-laundering language is significant because it requires financial institutions to set up their own due diligence to combat money laundering, particularly for private and corresponding banking situations. This is a key provision of which I was proud to be a part. I am pleased we were able to come up with language that allows that.

The amendment I advocated urges the Treasury Secretary to issue regulations ensuring these concentration accounts identify by client name all of the client funds moving through the account to prevent anonymous movement of the funds that might facilitate money laundering. This is a classic case of where this is so important. Raul Salinas, brother of Mexico's President Carlos Salinas, transferred almost $100 million to Citibank administrative accounts in New York and London without any documentation indicating the ownership of these funds. The wire transfers sent the funds to Citibank and asked each transfer be brought to the attention of a specific private banker. Later, the private banker transferred the funds to private bank accounts controlled by the Salarqis. The origin of this money—$100 million—was never satisfactorily identified.

Allegations of drug money or other corporate sources persist to this day. We believe, through Senator LEVIN's exhaustive documentation at his hearings, that other private banks use this practice as well. Although financial regulators have cautioned against this practice over and over again, they have not yet issued regulations to stop this loophole. That is why the language in this bill is so important.

The use of these anonymous concentration accounts breaks the audit trail associating specific funds with specific clients. The goal, as the President said, is to follow the money. We have to have information if we are going to follow the money.

If it should now be abundantly clear to the Treasury that they have the authority to stop, as well, what we have also abundantly clear it is a serious problem. I am very concerned that the administration act quickly on these anonymous accounts.

I congratulate everyone involved in this bill. I think our financial institutions, particularly the anti-money-laundering language is a critical part of making sure we have an effective antiterrorism bill. I thank my colleagues for their work.

The PRESIDING OFFICER. The time of the Senator from Michigan has expired. Who yields time?

The Senator from Wisconsin.

Mr. FEINGOLD. Mr. President, I will give a brief statement before I start my amendments, and I ask unanimous consent that I be divided amongst the time I have on each of my four amendments.

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

Mr. FEINGOLD. Mr. President, 1 month ago, we all were viciously attacked. I am pleased and grateful that both the domestic and international effort to respond to these attacks is fully underway. As we recall, almost as soon as the attacks of September 11 ended, our public discussion turned to two issues: how the United States will respond to these terrorist acts and how we can protect ourselves against future attacks.

Almost immediately, discussion of that second issue raised the question of how our efforts to prevent terrorism will affect the civil liberties enjoyed by all Americans as part of our constitutional birthright.

I was encouraged by many of the reactions that our leaders and Members of this body have had. Senator Allen, so increasingly encouraged by the words of our colleague, Senator GEORGE ALLEN of Virginia who represents one of the States struck by
terrorism. On the day after the attacks he said:

We must make sure that as we learn the facts, we do not allow these attacks to succeed in tempting us in any way to diminish what makes us a great nation. And what makes us a great nation is that this is a country that understands that people have God-given rights and liberties. And we cannot—none of us is to bring justice—diminish those liberties.

I agree with Senator ALLEN. I believe that one of the most important duties of this Congress is in responding to the terrible events of September 11th, in order to protect our civil liberties, which, of course, derive from our Constitution. That is why I am pleased that we did not take the Attorney General’s advice to enact an anti-terrorism bill immediately without any deliberation. I am pleased that we were able to reach agreement on a process that will allow some of my concerns with this bill to be debated and voted on through the amendment process.

That is not to say that no measures to strengthen enforcement should be enacted. They should be. We need to do it. We need to do some very serious updating of a number of these laws. This bill does many things to assist the Department of Justice in its mission to catch those who helped the terrorists and prevent future attacks. We can and will give the FBI new and better tools. But we must also make sure that the new tools don’t become instruments of abuse.

There is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country where the police were allowed to search your home at any time for any reason; if we lived in a country where the government was entitled to open your mail, eavesdrop on your phone conversations, or intercept your email communications; if we lived in a country where people could be held in jail indefinitely based on what they write or think, or based on mere suspicion that they might have the capacity to do great harm, then our government would probably discover and arrest more terrorists, or would be terrorists, just as it would find more lawbreakers generally. But that would not be a country in which we would want to live, and it would not be a country for which we could, in good conscience, ask our young people to fight and die. In short, that country would not be America.

I think it is important to remember that the Constitution was written in 1789 by men who had recently won the Revolutionary War. They did not live in comfortable and easy times of hypothetical enemies. They wrote the Constitution and Bill of Rights to protect individual liberties in times of war as well as in times of peace.

There have been periods in our nation’s history when civil liberties have taken a back seat to what appeared at the time to be the legitimate exigencies of war. Our national consciousness still bears the stain and the scars of those events: The Alien and Sedition Acts, the suspension of habeas corpus during the Civil War, the internment of Japanese-Americans during World War II and the injustices perpetrated against German-Americans and Italian-Americans, the blacklist in the McCarthy era, and the surveillance and harassment of antiwar protesters, including Dr. Martin Luther King, Jr., during the Vietnam war. We must not allow this piece of our past to become prologue.

Preserving our freedom is the reason we are now engaged in this new war on terrorism. We will lose that war without a shot being fired if we sacrifice the liberties of the American people in the belief that by doing so we will stop the terrorists.

That is why this exercise of considering the administration’s proposed legislation and fine tuning it to minimize the infringement of civil liberties is so necessary and so important. And this is a job that only the Congress can do. We cannot and must not rely on the Supreme Court to protect us from laws that sacrifice our freedoms. We took an oath to support and defend the Constitution of the United States. In these difficult times that oath becomes all the more significant.

There are quite a number of things in this bill that I am concerned about, but my amendments focus on a small discrete number of items.

At this point, I would like to turn to one of the amendments. The PRESIDENTING OFFICER. The Senator is recognized.

AMENDMENT NO. 1899

Mr. FEINGOLD. I send an amendment to the desk and ask for its immediate consideration.

The PRESIDENTING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Wisconsin [Mr. FEINGOLD] proposes an amendment numbered 1899.

Mr. FEINGOLD. I ask unanimous consent the reading of the amendment be dispensed with.

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

The amendment is as follows:

(Purpose: To make amendments to the provisions relating to interception of computer trespass communications.)

On page 42, line 25, insert “or other” after “contractual”.

On page 43, line 2, strike “for” and insert “permitting”.

On page 43, line 8, insert “transmitted to, through, or from the protected computer” after “computer trespasser”.

On page 43, line 20, insert “does not last for more than 96 hours and” after “such interception”.

Mr. FEINGOLD. I ask this time now to be charged to the first amendment.

The PRESIDENTING OFFICER. (Ms. STABENOW). The time will be charged.

Mr. FEINGOLD. Madam President, this amendment simply clarifies the provision in the bill dealing with computer trespass, section 217, so that it more accurately reflects the intent of the provision, as frequently expressed by the administration. Section 217 is designed, we have been told, to permit law enforcement to assist computer owners who are subject to denial of service attacks or other episodes of computer crime. As currently drafted, however, this provision could allow universities, libraries, and employers to permit government surveillance of people who are permitted to use the computer facilities of those entities. Such surveillance would take place without a judicial order or probable cause to believe that a crime is being committed.

Under the bill, anyone accessing a computer “without authorization” is deemed to have no privacy rights whatsoever, with no time limit, for as long as they are accessing the computer at issue. Basically, the way I read this, this provision completely eliminates fourth amendment protection for a potentially very large set of electronic communications.

The danger that this amendment tries to address is that “accessing a computer without authorization” could be interpreted to mean a minor transgression of an office or library computer use policy. Let’s take an example. Working mom uses an office computer to purchase Christmas presents on the Internet. Company policy prohibits personal use of office computers. This person has potentially accessed a computer without authorization and her company would give permission to law enforcement to review all of the e-mails that she sends or receives at work, monitor all the instant messages she sends, and record every website she visits: No warrant, no probable cause, no four amendment rights at all. My amendment makes clear that a computer trespasser is not someone who is permitted to use a computer by the owner or operator of that computer.

This amendment also limits the length of unreviewed surveillance to 96 hours, which is a longer time frame than that placed on other emergency wiretap authorities. Again, if
this provision is aimed solely at responding to cyber-attacks, there is no need to continue such surveillance beyond 96 hours—which is the time we put in our amendment—because that time is sufficient to allow the government to obtain a warrant to continue the surveillance. It is not fair to the owner or operator of the computer to find out later that he or she is not the target of government surveillance merely because they disobeyed a rule of the computer labs or student centers. Students use computers at school in the same way that people use computers at libraries. The need for immediate and emergency assistance during a denial of service attack or hacking episode, which I certainly think is a legitimate concern, cannot justify continued surveillance without judicial supervision.

Finally, this amendment prevents law enforcement from abusing this authority in investigations unrelated to the actual computer trespass. The current provision potentially allows law enforcement to intercept wire and electronic communications in many investigations where they may not want, or be able, to secure a court order. If the government suspects a person of committing a crime but does not have probable cause to justify monitoring of the suspect’s work computer, it could pressure the owner or operator of the computer to find some transgression in the suspect’s computer use, allowing the government carte blanche access to email and internet activity of the suspect. I suspect that few small business owners will be anxious to stand up to federal law enforcement requests for this information.

Now the administration was apparently willing to add language to deal with employees using office computers, but it refused to recognize that in our society many people use computers that they do not own, with permission, but without a contractual relationship. People own their own homes, but they use computers at libraries. Students use computers at school in computer labs or student centers. Without my amendment, these innocent users could become subject to intrusive government surveillance merely because they disobeyed a rule of the owner of the computer concerning its use. I have been told that this is not the administration’s intent, but they would not fix this provision. So I think it is fair to ask why. Why does the administration insist on leaving open the possibility that this provision will be abused to entirely eliminate the privacy of students’ and library patrons’ computer communications? Is there a hidden agenda here? I sincerely hope not, but I was very disappointed in the administration’s unwillingness to address this concern. I remain willing to negotiate on this amendment, but if there is no further movement on it, I hope my colleagues will recognize that this amendment will leave the publicly expressed concern of the public that the pass provision untouched and fix a potentially disastrous case of overbreadth.

I reserve the remainder of my time. I ask for the yeas and nays on the amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There is a sufficient second.

The yeas and nays on the amendment have been ordered printed.

Mr. FEINGOLD. Madam President, how much time do I have remaining on my side?

The PRESIDING OFFICER. Eighteen and one-half minutes on this amendment.

Mr. FEINGOLD. Madam President, I yield 5 minutes to the Senator from Washington.

The PRESIDING OFFICER. The Senator from Washington is recognized.

Mr. CANTWELL. Madam President, I rise to support my colleague, Senator FEINGOLD, and his amendment to section 217. I think the Senator has done a tremendous job in outlining the issues related to this bill and the fact that have come to light.

Haste in some instances on very well crafted language to uphold our rights under the Constitution can be infringed upon.

Section 217 is intended to allow computer system owners and operators to fully engage Federal law enforcement where someone hacks or intrudes into their system. As Senator FEINGOLD mentioned, that could be a business owner, or it could be a library system, or it could be a university system.

Unfortunately, as drafted, there are few limits on what communications the Government could intercept without showing probable cause that a crime has been committed and without having the opportunity for judicial review of those intercepts.

The provisions do not even limit the scope of the surveillance. Once authorized, the Government could intercept all communications of a person who is allegedly a trespasser. Again, let me be clear: without setting the fourth amendment requirement to show probable cause.

Further, there is no time limit on the surveillance under the provision of this legislation. For those who may be reviewing this legislation for the first time, and understanding that as they go to their workplace, or as they go to their educational institution, or as they go to their library to enhance their education, they could be under surveillance for a very long and indefinite period of time without their knowledge.

Thus, once authorized by a computer system operator, the Government could intercept all communications of a person forever without a proper search warrant. Even a court order wiretap expires after 30 days.

This amendment would remedy some of the defects in this bill. It would do that by requiring that the surveillance be only of communications associated with electronic trespass and that the length of the surveillance be limited to 96 hours, which, by the way, is twice as long as the time limit placed on emergency wiretap authority. If the problem continues, investigators could easily obtain additional warrant time for the surveillance to continue.

This is a very important time in our country’s history. It is a time in which the FBI has to act in urban and support the administration. It is a time in which we want to act to give law enforcement the tools they need to apprehend those who have been responsible and may be responsible for future acts of terrorism. But we also must preserve the rights of citizens of this country when it comes to the fourth amendment.

I encourage my colleagues to support the Feingold amendment. I yield the floor.

The PRESIDING OFFICER. Who yields time?

Mr. FEINGOLD. Madam President, first, I want to say how important it is to have on the committee the Senator with expertise in this area as well as Senator from Wisconsin. Let’s put a lot more much her help on this matter.

Madam President, how much time do I have remaining on my side?

The PRESIDING OFFICER. The Senator has 14 minutes.

Mr. FEINGOLD. I am happy to yield 5 minutes to the Senator from Minnesota.

The PRESIDING OFFICER. The Senator from Minnesota.

Mr. WELLS. Madam President, my colleague from Washington I think speaks within a framework of expertise that she brings to this particular amendment. I speak from the framework of a layperson who has been trying to understand this bill’s plusses and minuses.

I say to Senator FEINGOLD and all colleagues, since I think there is kind of a rush to table all of the Feingold amendments, that this amendment is eminently reasonable. The Senator from Wisconsin is saying: Let’s put a time limit on this. That is good. Let’s have some judicial oversight. That is good as well.

There are international terrorists who have killed many Americans and we want to kill more Americans. There are a lot of provisions in this bill which I think are right on the money, including northern border protection which is relevant to the Chair, relevant to the Senator from Washington, and certainly relevant to the people I represent. But I also think there is no reason, in this rush to pass the bill, that we can’t make some changes. These are minor changes the Senator wants to make. This just gives this piece of legislation more balance.

I will say this: There is a lot that is good in this bill and a lot that is attractive to me as a Senator. When you add some of the additional security provisions that help all the people we are asked to represent in addition to the financial help to all of the rescue workers and all of the innocent people’s families, people have been murdered—there is much in this
bill that is commendable. The Senator from Wisconsin is just trying to give it more balance.

I say to my colleagues that I hope you will support this amendment. I want to say one other thing as well. I really believe what we are good about in this bill is the provisions that focus on the people whom the terrorists are basically trying to kill—Americans. What is not as good as when the reach of the bill goes too far beyond that and that is too broad.

The sunset provision that passed in the Senate is so important, so that we can continue to monitor this legislation as we move forward.

I think this amendment that the Senator from Wisconsin has submitted is a step to give this piece of legislation a little more balance, and it will be more vigilant of people’s civil liberties. I think it is the right step. I thank the Senator for his amendment.

Mr. FEINGOLD. I thank the Senator from Minnesota for his help, especially for making this point: All this amendment does is taking sure that we are about the problem we face with the terrorism that is threatening our country and our freedoms. That is all we are trying to do—make sure it doesn’t go broadly into people’s rights, and into their privacy, and into their own lives. At this point, I am simply going to reserve the remainder of my time.

The PRESIDING OFFICER. Who yields time?

Mr. FEINGOLD. Madam President, let me talk a little bit about the provision of today’s legislation that has been referred to as the “computer trespasser” exception.

This provision is a perfect example of how our laws dealing with electronic surveillance have become outdated, and nonsensical as applied to modern technology.

Imagine the following scenario. A terrorist decides to wreak havoc in a major city by shutting down an electrical power grid. He uses a computer to hack into the mainframe computer of a regional utility company, which he plans to use to bring down the power grid. Before the terrorist can accomplish his goal, the utility company recognizes that an intruder is attempting to access their computer. The company quickly calls the FBI for assistance in repelling the intruder.

Guess what? Under current law, even with the permission from the utility company, the FBI is not permitted to monitor the terrorist’s activity on the utility company’s computer, because current law perversely grants the terrorist privacy rights with respect to his communications on the computer he has invaded.

It is anomalies such as this, in our current laws regarding electronic surveillance, that today’s legislation is designed to fix.

As it stands, the computer trespasser provision is defined in such a way that the owner or operator of a computer network cannot arbitrarily declare the user of a computer trespasser, and then invite law enforcement in to monitor that user’s communications.

The provision, as written, provides that a person is not considered a computer trespasser if the person has an “existing contractual” relationship for access to all or part of the computer network.

Senator FEINGOLD’s amendment would broadly amend the negotiated exception, including within its scope anyone with a contractual or “other” relationship to the owner or operator of a computer network. What is meant by “other” relationship? Any hacker could make the argument that they have a relationship with a computer operator. Indeed, were I a defense counsel, I would surely argue that the hacker has accessed the computer has created some form of relationship. Clearly, the proposed amendment would broadly and unwisely give immunity from our cyber-crime laws. This amendment would give the hacker the defense—this provision as it relates to the criminal laws and puts law enforcement back in the same position they currently are—that is, powerless to investigate hacking incidents where the owner of the computer network wants the assistance of law enforcement.

Madam President, we should not tie the hands of our law enforcement to assist the owners of our computer networks. We should not help hackers and cyberterrorists to get away. If you are a victim of a burglary, shouldn’t you have the right to ask the police to investigate your house, to come to your house and investigate?

Why should the owners of the computer not have the right to ask the police to investigate a computer-hacking incident, especially where it appears it is terrorist-oriented?

This act applies, as written, only to people without authorization to be on the computer. Why should the law protect people who have invaded a computer they have no right to be on?

Let me say one last comment about this. The proponents of this amendment argue it will apply to students using a university computer. That is true, but only if such students use that university computer to hack into a place where they do not belong.

Either we have to get serious in this modern society, with these modern computers, about terrorism or we have to ignore it. I, for one, am not for ignoring it. I believe we need to have this language in here—so does the Justice Department; so does the White House and the White House Counsel’s Office—in order to do what cannot be done today, protect people in our society, and to protect our powerplants, our dams, and so many important facilities in our society that are vulnerable to cyber-terrorists. This law, the way it is currently written, will help to do that.

That is all I care to say about it. But I believe we should vote down the Senator’s amendment. I know it is well intentioned. I have great respect for the Senator from Wisconsin. He is one of the very diligent members of this committee, and I appreciate him very much, but on this amendment I believe we have to keep the language of the bill the way it is written in order to give our law enforcement people the tools to be able to stop terrorist hacking into computers.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. I thank my friend for his kind words.

Madam President, in response to the points he made, first, let me respond that I accept the premise of this basic provision in terms of updating the ability to get at computer hackers. That is an update. We did not know what this was going to be years ago. I know what risks it posed. Nobody opposes that very important part of this bill.

But what the Senator claims is that the phrase “contractual relationship” somehow makes sure that people are protected from being found guilty for what risks who really should not be subject to this, but it does it.

I can think of at least three categories of people who do not come within the category of “contractual relationship.” One is employment. It is nice if you have a contract, but a lot of employees do not. They do not fall within the protection of a contractual relationship.

The same goes for people who would go and use a computer at a library. They do not have a contractual relationship to protect them in this situation.

And finally, as the Senator conceded here, in his last example, that certain students, students at all our universities across the country, are not protected by that language. And that is all we want to do, to make it clear that this amendment is related to the problem of computer hackers, not moms who might be buying Christmas presents on a computer at work, even though they are not supposed to, or students who maybe are gambling on a university computer. Of course they should not do that, but should that somehow protect students from the legal intrusion by Government law enforcement authority? Of course not.

The Senator attempts to suggest that the provision in here having to do with our desire to have the language say “contractual” or “other” relationship. I repeat from the Senator to claim that he is protected. The notion that a hacker would be considered as somebody who has a relationship with the company under this amendment is an absurd interpretation of the amendment. The Senator really is not what this amendment would do.

And finally, let me get back to the students, the example the Senator
from Utah mentioned. It is simply an unprecedented intrusion into individual rights for a university to be able to allow—because of a minor use that is not within university rules—that person to be completely subject to this kind of intrusion.

Mr. DURBIN. Will the Senator yield for a question?

Mr. FEINGOLD. Yes.

Mr. DURBIN. I have followed this debate closely. I commend the Senator for his leadership on the constitutional rights part of this debate. But I want to make sure I understand exactly what his amendment sets out to do.

Is my understanding correct that under the Feingold amendment there could be surveillance of a computer for 96 hours before there is any court approval, so that in the example given by the Senator from Utah, the law enforcement authorities could, in fact, monitor the communications of someone who had access to the computer for 96 hours before ever going to a court and asking for a warrant for that search?

Mr. FEINGOLD. That is correct. And that even troubles me for the length of time that it is allowed—but it is far better than the position. Law Enforcement should be required to seek a warrant as soon as possible, within reason, given the fact that what the amendment tries to get at is emergency situations involving hackers. As soon as possible, they should have to meet the standards that are normally met.

But, yes, the amendment does permit that, in my view, rather extraordinary period of time before the requirement would have to be made.

Mr. DURBIN. And that period of time, I ask the Senator from Wisconsin, is roughly twice the amount currently given under emergency wiretap authority; is that correct?

Mr. FEINGOLD. No, my time is correct.

Mr. DURBIN. One last question. I want to try to understand. I ask the Senator do you not say, in your amendment, that a trespasser does not include someone who is permitted to use a computer by the owner or operator of the computer?

Mr. FEINGOLD. Correct.

Mr. DURBIN. And the difference, of course, is whether it is a contractual relationship or just a permission to use; you are including permission to use as well as contractual relationship?

Mr. FEINGOLD. That is correct.

Mr. DURBIN. The examples you have given are of people going to a library, who may not have a contractual relationship with the library but use the computer, who would be subjected to this warrantless search of their computer communications for an indefinite period of time.

Mr. FEINGOLD. That is right, exactly. This is exactly the problem. All we asked of the committee and of the administration yesterday was to make it clear that they did not want to reach these people. That is what we have been told. The purpose of this is to get at the threat of computer hackers.

The Senator from Illinois has just illustrated, with those examples—and he is, of course, correct—that this could be interpreted and could be understood to include situations that not only have minor situations that not only have minor monetary issues but represent a very serious departure from the individual rights people should have in our country.

Mr. DURBIN. I thank the Senator from Wisconsin.

Mr. FEINGOLD. I thank the Senator from Illinois and reserve the remainder of my time.

Mr. LEAHY. Madam President, I have been concerned about the scope of the amendment carving an exception to the wiretap statute for so-called “computer trespassers.” This covers anyone who accesses a computer “without authorization” and could allow government eavesdropping, without a court order or other safeguards in place. I believe the bill as written, for example, users who violate workplace computer use rules or online service rules.

I was unable to reach agreement with the administration on limiting the scope of this amendment, and the Feingold amendment makes further refinements. It is unfortunate that the administration did not accept this amendment.

The PRESIDING OFFICER. Who yields time?

Mr. HATCH. Madam President, how much time remains?

The PRESIDING OFFICER. The Senator from Pennsylvania.

Mr. SPECTER. Madam President, I ask the chairman of the committee, after listening to the presentation by the Senator from Wisconsin, what is the chairman’s view of the incursion on law enforcement by the limitation of 96 hours?

Mr. LEAHY. The incursion of law enforcement by the 96 hours?

Mr. SPECTER. The principal thrust of what the Senator from Wisconsin seeks to do is to broaden the definition of a contractual relationship to someone who may otherwise have permission. What I am trying to do is to understand the administration’s position, the law enforcement position as to how law enforcement is adversely impacted by what the Senator from Wisconsin seeks to do.

My concern, as expressed earlier, is that, especially in the face of the challenge by the amendment, this is a complicated bill.

The reality is, it is hard to know all of it without the normal hearing process. Now we have a specific challenge. What I would like to know is, how does it inhibit law enforcement? What about the Senator’s concerns about problems to law enforcement? And then, what is the difficulty in having 96 hours, which is 4 days, to see what is going on to find some basis for seeking a warrant with probable cause?

Mr. LEAHY. Frankly, I don’t have a problem with the Feingold amendment as it is written. I do have a problem, however, with keeping a bill together. The initial administration request had no limitations whatsoever. It was so wide open we were concerned that someone who might be using a computer at work to add up their accounts for the month would be trapped by this because the company said you couldn’t use the computer to add up your checkbook. They limited it to the length of time that it is allowed back where we are when we can’t do anything.

The administration moved partly our way and actually ended up with a compromise on this. I suspect what they would say to the Senator from Pennsylvania is that these attacks last more than 96 hours and that they would be unable to go after them if they were limited to the 96 hours.

We saw this recently 2 or 3 weeks ago where we had a continuous roving attack on a number of Government computers. As I recall—I didn’t pay that much attention at the time—they were attacking them one week and when we came back the following week, they were still attacking them. So you had more than 96 hours.

Frankly, it is a case where we have reached a compromise. The distinction is, and Frankly, I am not speaking on behalf of the administration, said this is not acceptable to them. Had this been part of the original package, I wouldn’t have found it acceptable.

Mr. HATCH. Will the Senator yield?

Mr. SPECTER. Yes.

Mr. HATCH. Basically, what the administration is after here is that if a burglar is coming into your home and the police come to investigate, they don’t have to report to a judge within 96 hours. The police are tasked on these terrorist matters. If they find that a terrorist has infiltrated a computer controlling an electrical grid system, they want to get right on the ball and do something about it. That is what they are trying to do with this provision.

There are no fourth amendment rights implicated because you have people who have hacked into a computer that they don’t have any right to be in.

We want to give law enforcement the power to stop that. This provision upsets that power and basically puts us back where we are when we can’t do
anything in a modern digital age to stop terrorists from stopping power grids and damaging dams and a whole raft of other things.

Mr. SPECTER. Madam President, if the Senator from Utah will yield for a question?

Mr. HATCH. Surely.

Mr. SPECTER. The Senator from Wisconsin makes the point that people may have standing to use a computer even without a contractual relationship, uses the example of a student. Does the Senator from Utah believe or does the administration represent that there are no relationships other than contractual which give a person the legitimate standing to use the computer?

Mr. HATCH. Under this provision, you do not have a right to hack into another private computer, whether you are a university student or anybody else. It only applies, the law we have written, to unauthorized access. It does not apply to authorized access. But unauthorized access, yes, it applies to that. If we don’t put it in there, we will be leaving a glaring error that currently exists in our laws that prohibit us from solving some of these problems. It would be a terrible thing to not have at this particular time, knowing what we know about how these terrorists are operating right now.

Mr. SPECTER. So is the Senator from Utah saying that if you have permission that it is not a form of a contractual relationship?

Mr. HATCH. I am saying that if you have permission, you are not covered by this provision as written. In other words, you would not be considered a hacker?

Mr. SPECTER. On its face you would seem to, unless there is a contractual relationship?

Mr. HATCH. It comes down to authorized or unauthorized access. If it is authorized access, it is not covered under the computer trespasser provision.

Mr. SPECTER. I thank the Senator. The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Madam President, did the Senator yield back his remaining time?

Mr. HATCH. Yes, we are prepared to yield.

Mr. LEAHY. We are prepared if the Senator from Wisconsin is.

Mr. SPECTER. I want to clarify a couple points. First of all, it became very clear from Senator Specter’s excellent questioning that, of course, there is no guarantee, under the way this language is set up, under the words “contractual relationship,” that the provision would not apply to students or to people who would use a computer at a library. I can’t understand why, if that is true, the language of the amendment, the intent of the legislation, why they don’t just agree to language that would say so. That is all we asked for yesterday. It could have resolved the problem. For some reason, they won’t agree to it.

Second, is this notion that a hacker could somehow get in under our language. There is no way that a hacker has a relationship with the computer owner even in the case of the use of the computer. The hacker is, obviously, the antithesis, the opposite of an individual with a relationship that permits use of the computer.

Finally, I am amazed at this notion that this amendment, even under our version of it, would allow only 96 hours for surveillance when under the example of the Senator from Utah, an ongoing hacker attack is occurring.

Is it the Senator’s contention that at the end of 96 hours, the FBI would not have probable cause to get a warrant, when all it has been dealing with for 4 days is this hacking of the computer? Of course, it would. It would be the easiest thing in the world.

Section 424(a) requires an affidavit stating a justification under the computer trespasser provision.

Mr. SPECTER. The Senator from Utah will yield for a question?

Mr. SPECTER. I want to respond to the Senator from Wisconsin. As the Senator from Utah, or a Colorado senator?

Mr. SPECTER. No, from Wisconsin. The hacker is, obviously, the antagonist of an owner that permits the use of the computer. The hacker is, obviously, the antithesis of the individual with a relationship that permits use of the computer.

Mr. HATCH. As the Senator from South Dakota, the reason why the Senator from Utah is so concerned about an amendment with which he would be sympathetic, he would put it in there.

Mr. DASCHLE. Madam President, I have listened to this debate with great interest, and I appreciate very much the Senator from Utah, who has a stronger commitment to our individual rights and personal liberties than the senior Senator from South Dakota, our majority leader. But I also know that were it not for his commitment and efforts, we would not have been here to deal with the bill. In my judgment, what became clear is the wisdom of this approach, to move away from the notion that a warrant is required in every circumstance, but also to have a provision that would most likely occur in such a circumstance.

I hope my colleagues will join me tonight in tabling this amendment and tabling every other amendment that is offered, should he choose to offer them tonight. Let’s move on and finish this bill. Let’s work with the House and come up with the best product between the Houses. Then, let’s let law enforcement do its job, and let’s use our power of oversight to ensure that civil liberties are protected.

Now, if we had opened the bill to amendment, I have no doubt there are many colleagues who would offer amendments with which I would vehemently disagree—in fact, so much so that I might want to filibuster the bill. I would probably lose. I think there is a realistic expectation that on a lot of these issues, my side would lose. I think we should make the best case for the other side. So, we made the best judgment we could, taking into account the very delicate balance between civil liberties and law enforcement that we had to achieve in bringing this bill to the floor.

I have to say, I think our chair and ranking member and all of those involved did a terrific job under the most difficult of circumstances. What we did was to say: Let’s take this product and work with it; let’s review it; if we have to make some changes, let’s consider them; but let’s recognize that if we were to take this bill open-ended, there would be no end to the amendments—

Mr. SPECTER. The amendment that would most likely occur in such a circumstance.

Given those circumstances, my argument is not substantive, it is procedural. We have a job to do. The clock is ticking. The work needs to get done. We have to make our best judgment and get it done. I will make a motion to table.

Mr. LEAHY. Will the Senator withdraw that motion to table for a moment?

Mr. DASCHLE. Yes.

Mr. LEAHY. Madam President, I have served with over 250 Senators here, and I have been proud to serve with all of them. I know of no Senator who has a stronger commitment to our individual rights and personal liberties than the senior Senator from South Dakota, our majority leader. But I also know that were it not for his commitment and efforts, we would not be here with a far better bill than the one originally proposed by the administration, that has been because of his willingness to back us up as we try to improve that bill, to remove unconstitutional aspects of it, because of his willingness, we were able to get here.

As the Senator from South Dakota, the best friend I have in this body, he could have done differently, and he knows there are parts I would do differently—even on this one. I have high regard for the
Senator from Wisconsin, and I would have loved to have had his amendment. Actually, I would have done it probably differently than that. But we had a whole lot of places where we won and some where we lost.

I could tell you right now, if we start unraveling this bill, we are going to lose all the parts we won and we will be back to a proposal that was blatantly unconstitutional in many parts. So I join, with no reluctance whatsoever, in the leader's motion.

Mr. DASCHLE. Madam President, I move to table.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Madam President, on this bill there was not a single moment of markup or vote in the Judiciary Committee. I accepted that because of the crisis our Nation faces.

This is the first substantive amendment in the Senate on this entire issue, one of the most important civil liberties bills of our time, and the majority leader has asked Senators to not vote on the merits of the issue. I understand the difficult task he has, but I must object to the idea that not one single amendment on this issue will be voted on the merits on the floor of the Senate.

What have we come to when we don't have either committee or Senate deliberation on amendments on an issue of this importance?

yield the floor, and I yield back the remainder of my time.

The PRESIDING OFFICER. All time is yielded back.

Mr. DASCHLE. Madam President, I move to table the amendment.

Mr. LEAHY. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There is a sufficient second.

The question is on agreeing to the motion.

The clerk will call the roll.

The legislative clerk called the roll.

Mr. NICKLES. I announce that the Senator from North Carolina (Mr. HELMS), the Senator from New Mexico (Mr. DOMENICI), the Senator from South Carolina (Mr. THURMOND), and the Senator from Mississippi (Mr. LOTT) are necessary absent.

I further announce that if present and voting the Senator from North Carolina (Mr. HELMS) would vote "yea.

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 83, nays 13, as follows:

[Rollcall Vote No. 219 Leg.]

YEAS—83

Mr. FEINGOLD. I ask unanimous consent reading of the amendment be dispensed with.

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

The amendment is as follows:

On page 21, line 14, insert "except that, in such circumstances, the order shall direct that the surveillance shall be conducted only when the target's presence at the place where, or use of the facility at which, the electronic surveillance is to be directed has been ascertained by the person implementing the order and that the electronic surveillance must be directed only at the communication of the target," after "such other persons".

Mr. KERRY. For the purpose of planning, could the Senator give us a sense of both amendments and how long he thinks he will talk.

Mr. FEINGOLD. I have about 12 minutes on this amendment subject to any response to that and approximately the same on the second amendment.

Mr. KERRY. I thank the Chair.

Mr. FEINGOLD. Madam President, this amendment has to do with what is called roving wiretap, or multipoint surveillance authority. This is one of the first things Attorney General Ashcroft asked for in the first days after the September 11 attack and gave the example of a terrorist using throw-away cell phones and the need for continuing roving wiretap authority to allow the FBI to keep up with the ready availability of this new technology.

First, let me say I have a lot of sympathy for the idea of updating this area of the law. Obviously, it is needed in light of changes in technology. It is vitally important for Members of the Senate to understand that roving wiretap authority is already available for criminal investigations under Title III. It is in title 18, section 2518(11) and (12), The Attorney General doesn't need nor has he asked for any new roving wiretap authority for criminal investigations, He already has it.

That the bill does, Section 206 is provide similar authority in investigations under the Foreign Intelligence Surveillance Act, known as FISA. I am not opposed to expanding existing roving wiretap authority to include FISA investigations, but I am very concerned that Section 206 does not include a key safeguard that was part of the roving wiretap authority when it was added to title III in 1986. That protection minimizes the possible misuse of the authority, whether intentional or unintentional, to eavesdrop on the conversations of individuals who are not the subject of the investigation.

Let me read from the Senate Judiciary Committee's report on the legislation that granted roving wiretap authority:

Proposed subsection 2518(12) of title 18 provides, with respect to both "wire" and "oral" communications, that no government has been successful in obtaining a relaxed specificity order, it cannot begin the interception until the facilities or place from which the communication is to be intercepted is ascertained by the person implementing the interception order.

Mr. KERRY. Madam President, it is my intention to offer two more amendments, not the third amendment.

I yield 5 minutes to the Senator from Utah and I have and we have committed to Senators on both sides of the aisle who need time.

The remaining time is for the Senator from Wisconsin who has three more amendments with the same time as he had in the last amendment.

The Senator from Massachusetts has asked for 5 minutes. I understand we have three more amendments that would take probably an hour or so per amendment with the vote if the Senator from Wisconsin wishes to use all his time, and he has a right to do that. Once those are disposed of, the Senator from Utah and I are probably prepared to yield back our time.

I yield 5 minutes to the Senator from Massachusetts.

Mr. LEAHY. Madam President, it was depending entirely on what the Senator from Wisconsin was doing. I reserve that now and see where we are heading.

Mr. LEAHY. I yield the floor.

Mr. FEINGOLD. Madam President, it is my intention to offer two more amendments, not the third amendment. I believe the time for each of those amendments could be less than the full time allotted. We have a fair amount of interest, but I didn't expect as much debate. I think the last two could be expedited, and I am prepared to proceed, if that is what my colleagues desire.

The motion was agreed to.

Mr. LEAHY. I move to reconsider the vote.

Mr. DASCHLE. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

Mr. LEAHY. Madam President, so we understand where we are, there is still a fair amount of time on the bill that has from Utah and I have and we have committed to Senators on both sides of the aisle who need time.

The remaining time is for the Senator from Wisconsin who has three more amendments with the same time as he had in the last amendment.

The Senator from Massachusetts has asked for 5 minutes. I understand we have three more amendments that would take probably an hour or so per amendment with the vote if the Senator from Wisconsin wishes to use all his time, and he has a right to do that. Once those are disposed of, the Senator from Utah and I are probably prepared to yield back our time.

I yield 5 minutes to the Senator from Massachusetts.

Mr. KERRY. Madam President, it is depending entirely on what the Senator from Wisconsin was doing. I reserve that now and see where we are heading.

Mr. LEAHY. I yield the floor.

Mr. FEINGOLD. Madam President, it is my intention to offer two more amendments, not the third amendment. I believe the time for each of those amendments could be less than the full time allotted. We have a fair amount of interest, but I didn't expect as much debate. I think the last two could be expedited, and I am prepared to proceed, if that is what my colleagues desire.

I send an amendment to the desk and ask for its immediate consideration.
In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation.

It further reads:

It would be improper to use this expanded statutory authority for a series of phone calls among phone conversations. If the government uses this expanded statutory authority to monitor a new cell phone, it could and undoubtedly would, with current law, be using that phone again.

Mr. FEINGOLD. Yes. Madam President.

Mr. WELLSTONE. Again, I am not a lawyer. I do not think I understood exactly all the argument you were making.

Are you saying there has to be some standard of proof? That before conducting surveillance, law enforcement has to ascertain that the individual is actually there. Without that kind of rule, what we are doing is not just extending this authority to the reality that people have cell phones and move around and use different phones of their own, but it takes us into an area that, frankly, prior to September 11 we would have seen an open end to change it, but we didn’t. Even after the change made in 1999 without discussion or debate, the standard remains in effect for bugs placed in homes or businesses. Without this protection, Section 206 threatens the rights of innocent people.

If law enforcement has been significantly impaired in conducting effective surveillance in criminal investigations under the roving wiretap provision in current law, we should be shown specific evidence of its shortcomings. But if it has not been impaired, then there is no reason not to include a similar safeguard in the roving wiretap authority under FISA.

I urge my colleagues to take a close look at this amendment. It is reasonable, it appropriately reflects current law, but it also allows for updating to face the reality of new technology and all the technologies that are implicated here. And it protects the constitutional rights of people who are not the subjects of an investigation.

Mr. WELLSTONE. Will the Senator yield for a question?

Mr. FEINGOLD. Yes.

Mr. WELLSTONE. Again, I am not a lawyer. I do not think I understood exactly all the argument you were making.

Are you saying there has to be some standard of proof? That before conducting surveillance, law enforcement has to make sure? In other words, before you actually wiretap a phone or bug a house or a home, the target of the surveillance has to be in that home you are bugging?

Mr. FEINGOLD. No. Let’s say somebody goes to their neighbor’s house to talk on their phone. They don’t ever once or twice or whatever it might be. Our amendment makes sure this new provision doesn’t open up that house and everybody in it and every phone call they have in the house to unlimited Government surveillance. It requires what has been a normally required standard: that, because of the wiretap, that the law enforcement people ascertain that the person is in the house at the time so it is credible that they would be using that phone again.

Mr. WELLSTONE. In other words, other people who are in the house who have nothing to do with the target of surveillance, their conversations could be—

Mr. FEINGOLD. Their conversations could and undoubtedly would be, without this amendment.

Mr. WELLSTONE. And the same thing for the bugging?

Mr. FEINGOLD. Exactly.

Mr. WELLSTONE. So you are trying to minimize the misuse of authority. It may be unintentional?

Mr. FEINGOLD. Absolutely. There are standards, as I indicated in my statement. There have been rules about how law enforcement has to ascertain, whether it be at a phone bank or in somebody else’s home, that there is a reasonable belief that the individual is actually there. Without that kind of rule, what we are doing is not just extending this authority to the reality that people have cell phones and move around and use different phones of their own, but it takes us into an area that, frankly, prior to September 11 we would have never dreamed of allowing.

Mr. WELLSTONE. Madam President, if I could take 2 minutes—I ask the Senator from Wisconsin, might I have 2 minutes?

Mr. FEINGOLD. Yes. Madam President, I ask for the yeas and nays on the amendment.

The PRESIDING OFFICER. Is there a sufficient second? There appears to be. The yeas and nays were ordered.

Mr. FEINGOLD. I yield 2 minutes.

Mr. WELLSTONE. My colleague is saying we have to be very careful about not eavesdropping on the conversations of innocent individuals.

Again, we all are painfully aware of September 11. I personally think there is much in this bill that is good, that we need to do. But I think all the Senator from Wisconsin is trying to do is achieve some balance and make sure we do not go above and beyond going after terrorists who are trying to kill Americans and instead end up eavesdropping on innocent people in our country.

In other words, the vast majority of the people in the country, if they understood what this amendment was about, would support this amendment. I do not think passing this amendment does
any damage whatsoever to much of what is in this bill, which is so important.

So, again, I hope Senators will support this amendment on the merits. I think it is a very important amendment. I thank the Senator from Wisconsin.

Mr. FEINGOLD. I thank the Senator from Minnesota very much for his help, and I reserve the remainder of my time.

The PRESIDING OFFICER. Who yields time? The Senator from Utah.

Mr. HATCH. Madam President, under current law, law enforcement has so-called-roving or multi-point surveillance authority for criminal investigations under title III, but FISA does not have comparable provisions for agents investigating foreign intelligence. Roving interpretations are tied to a named person rather than to any particular communications facility or place. Today’s bill adds this vital authority to FISA.

This authority is critical for tracking suspected spies and terrorists who are experts in counter-surveillance methods such as frequently changing locations and communications devices such as phones and computer accounts.

It simply makes no sense that our wire-tapping statute recognizes this problem, and provides roving wiretap authority for surveillance of common criminals, but makes no provision for roving authority to monitor terrorists under the FISA statute.

The proposed amendment would not succeed in its stated goal of harmonizing the standard between title III wiretaps and FISA wiretaps. The proposed amendment would put a requirement on the interception of wire or electronic communications under a FISA warrant that does not exist in the title III context—a requirement that the law enforcement officer implementing the wiretapping order personally ascertain that the target of the order is using a telephone or computer, before the monitoring could begin.

This requirement is operationally unworkable. The way that roving orders are implemented, requires that law enforcement officers have the ability to spot check several different telephones in order to determine which one is being used by the target of the order. The language proposed in this amendment does not give law enforcement officers the ability to do so. In fact, they would be worse off under this proposal than they are under current law.

The goal of the roving wiretap provision is to give counter-terrorism investigators as much authority to conduct wiretaps as their counterparts have in conducting criminal investigations. This amendment defeats that goal by putting new, significant obstacles in the path of investigators attempting to investigate and prevent terrorist activities.

Mr. LEAHY. Madam President, Senator FEINGOLD provided invaluable assistance to the committee during our consideration of this legislation. He also held a hearing in his Constitution Subcommittee last week on the critical civil liberties issues raised by the Administration’s anti-terrorism bill. I fully appreciate the depth of his concern and his desire to improve this bill. The Senator from North Carolina I agreed that the principal, the roving, or multipoint, wiretap authority for criminal cases should be available under FISA for foreign intelligence cases. The need for such authority is especially acute to conduct surveillance of foreign spies trained in the art of avoiding surveillance and detection.

Senator FEINGOLD’s amendment simply assures that when roving surveillance is conducted, the Government makes efforts to ascertain that the target is actually at the place or using the phone, being tapped. This is required in the criminal context. It is unfortunate that the Administration did not accept this amendment.

I hope all time could be yielded back on both sides.

Mr. FEINGOLD. It is my understanding that the opponents have yielded all time.

The PRESIDING OFFICER. The Senator is correct.

Mr. LEAHY. If the Senator is going to yield his.

The PRESIDING OFFICER. The majority leader.

Mr. DASCHLE. Madam President, I will just use a minute of my leader time to respond.

I have already made my argument on the first amendment. I, in the interest of time, am not going to repeat it. As I said before, I am sympathetic to many of these ideas, but I am much more sympathetic to arriving at a product that will bring us to a point where we can pass something into law. The record reflects the compromises that have been put in place, that the very delicate balance that we have achieved.

It is too late to open up the amendment process in a way that might destroy that delicate balance. For that reason, I move to table this amendment.

I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second? There is a sufficient second.

The question is on agreeing to the motion. The clerk will call the roll.

The assistant legislative clerk called the roll.

Mr. NICKLES. I announce that the Senator from North Carolina (Mr. HELMS), the Senator from South Carolina (Mr. THURMOND), and the Senator from New Mexico (Mr. DOMENICI) are necessarily absent.

I further announce that if present and voting the Senator from North Carolina (Mr. HELMS) would vote “yea.”

The result was announced—yeas 90, nays 7, as follows:

<table>
<thead>
<tr>
<th>YEA—90</th>
<th>NAY—7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akaka</td>
<td>Dorgan</td>
</tr>
<tr>
<td>Allard</td>
<td>Doran</td>
</tr>
<tr>
<td>Allen</td>
<td>Durbin</td>
</tr>
<tr>
<td>Baucus</td>
<td>Edwards</td>
</tr>
<tr>
<td>Bayh</td>
<td>Ensign</td>
</tr>
<tr>
<td>Bennett</td>
<td>Feingold</td>
</tr>
<tr>
<td>Biden</td>
<td>Fitzgerald</td>
</tr>
<tr>
<td>Bingaman</td>
<td>Flaherty</td>
</tr>
<tr>
<td>Boxer</td>
<td>Graham</td>
</tr>
<tr>
<td>Бреаux</td>
<td>Grassley</td>
</tr>
<tr>
<td>Brown</td>
<td>Hagel</td>
</tr>
<tr>
<td>Burns</td>
<td>Harkin</td>
</tr>
<tr>
<td>Byrd</td>
<td>Hatch</td>
</tr>
<tr>
<td>Campbell</td>
<td>Hollings</td>
</tr>
<tr>
<td>Carabash</td>
<td>Hutchinson</td>
</tr>
<tr>
<td>Chafee</td>
<td>Inhofe</td>
</tr>
<tr>
<td>Cleland</td>
<td>Inouye</td>
</tr>
<tr>
<td>Clinton</td>
<td>Johnson</td>
</tr>
<tr>
<td>Cochran</td>
<td>Kennedy</td>
</tr>
<tr>
<td>Collins</td>
<td>Kerry</td>
</tr>
<tr>
<td>Conrad</td>
<td>Kohl</td>
</tr>
<tr>
<td>Craig</td>
<td>Kyl</td>
</tr>
<tr>
<td>Crapo</td>
<td>Landrieu</td>
</tr>
<tr>
<td>Daschle</td>
<td>Leahy</td>
</tr>
<tr>
<td>Dayton</td>
<td>Lieberman</td>
</tr>
<tr>
<td>DeVine</td>
<td>Lincoln</td>
</tr>
<tr>
<td>Dodd</td>
<td>Wyden</td>
</tr>
</tbody>
</table>

Mr. LEAHY. The motion was agreed to.

Mr. LEAHY. I move to reconsider the vote.

Mr. HATCH. I move that the motion on the table.

The motion to lay on the table was agreed to.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. Madam President, I ask unanimous consent to have printed in the RECORD a Statement of Administration Policy on the USA Act.

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

STATEMENT OF ADMINISTRATION POLICY
(Continued from page S10576)

S. 1510—UNITING AND STRENGTHENING AMERICA (USA) ACT OF 2001

The Administration commends the Senate leadership and the Chairman and Ranking Member of the Senate Judiciary Committee on reaching agreement on S. 1510. This bill contains, in some form, virtually all of the proposals made by the Administration in the wake of the terrorist attacks perpetrated against the United States on September 11th. The Administration strongly supports passage of this bill.

The Administration’s initial proposals, on which S. 1510 is based, were designed to provide Federal law enforcement and national security officials with the tools and resources necessary to disrupt, weaken, and counter the infrastructure of terrorist organizations, to prevent terrorist attacks, and to punish and defeat terrorists and those who harbor them. S. 1510 includes the provisions proposed by the Administration in three main areas: (1) information gathering and sharing; (2) substantive criminal law and criminal procedure; and (3) immigration procedures. The Administration strongly supports passage of these provisions. The Administration also supports valuable provisions, introduced by the Chairman of the
Senate Judiciary Committee, aimed at improving the Nation’s border protection.

**Information Gathering and Sharing**

Existing laws fail to provide national security authorities and law enforcement authorities with the critical tools they need to fight and win the war against terrorism. For example, technology has dramatically outpaced the Nation’s statutes. Many important intelligence gathering laws were enacted decades ago, in and for an era of rotary telephones. Meanwhile, the Nation’s enemies use e-mail, the Internet, mobile communications and voice mail.

S. 1510 contains numerous provisions that address this problem by helping to make the intelligence and surveillance statutes more “technology-neutral.” Specifically, the bill updates the pen-register, trap-and-trace, and Title III-wiretap statutes to cover computer and mobile communications more effectively, while ensuring that the scope of the authority remains the same.

The bill also provides for nationwide scope of orders and search warrants, and other practical changes that will enable law enforcement to work more efficiently and effectively. The bill contains important updates of foreign intelligence gathering-statutes, with the identical goal of making the statutes technology-neutral. Even the bill contains provisions to reduce existing barriers to the sharing of information among Federal agencies where necessary to identify and respond to terrorist threats. The ability of law enforcement and national security personnel to share this type of information is a critical tool for pursuing the war against terrorism on all fronts.

**Substantive Criminal Law and Criminal Procedure**

S. 1510 contains important reforms to the criminal statutes designed to strengthen law enforcement’s ability to investigate, prosecute, prevent, and punish terrorism crimes. The bill would remove existing barriers to effective prosecution by extending the statute of limitations for terrorist crimes that risk or result in death or serious injury. The bill also creates and strengthens criminal statutes, including a prohibition on harboring or giving material support to terrorists, and provides for tougher penalties, including longer prison terms and higher conspiracy penalties for those who obstruct such acts. These provisions will help to ensure that the fight against terrorism is a national priority in our criminal justice system.

**Border Protection and Immigration Procedures**

S. 1510 also contains a number of provisions that would enhance the ability of immigration officials to exclude or deport aliens who engage in terrorist activity and improve the Federal government’s ability to share information about suspected terrorists. Under the bill, those who contribute to or otherwise support terrorist organizations and terrorists would be considered illegal, and those would be deported from the United States. In addition, the bill provides for access by the Department of State and the Immigration and Naturalization Service to criminal history records and related information maintained by the Federal Bureau of Investigation.

**Money Laundering**

Title III of S. 1510 includes money laundering statutes, with the identical goal of strengthening the money laundering enforcement-statutes, with the identical goal of reducing the debt, fund priority initiatives, and grant tax relief to all income tax paying Americans.

**The PRESIDING OFFICER.** The Senator from Vermont.

**Mr. LEAHY.** Madam President, I know the Senator from Wisconsin has another amendment. I have had requests for time on our side of the aisle from the distinguished Senator from Washington State, Ms. CANTWELL, for 7 minutes; the distinguished Senator from Tennessee, Mr. SMITHERS, for 5 minutes; the distinguished Senator from Massachusetts, Mr. KERRY, for 5 minutes; the distinguished Senator from Minnesota, Mr. WELLSTONE, for 5 minutes; the distinguished Senator from Michigan, Mr. LEVIN, for 2 minutes.

I mention that, not to lock that in, because the time is there, but just to give people an idea of where we are.

**The PRESIDING OFFICER.** The Senator from Wisconsin.

**Mr. PEINGOLD.** Madam President, is the Senator from Vermont proposing a time agreement?

**Mr. LEAHY.** No. I am just saying what people are requesting for time. I am trying to get some idea. A number of Senators want to distin- guish themselves from the Majority Leader and myself and express their support of the President, that a terrorist act may happen in the United States or overseas in the next several days.

We do need adequate law enforce- ment powers. We should have finished this bill some time ago. But when the Majority Leader says he is concerned about procedure and not about substance, we are regretfully establishing a record where we have not only not shown the deliberative process to uphold constitutional scrutiny, but we are putting the President in the position of the majority leader in wanting to get this bill finished. Earlier this evening, I went through an elaborate chronology as to what has happened here. Nine days after September 11, the Attorney General submitted a bill. I had suggested hearings that week. The bill was sub- mitted on September 20. We could have had hearings on September 21 and even on September 22, a Saturday. The Judi- ciary Committee had one hearing, a very brief one, on September 22. I wrote the chairman of the committee two letters urging hearings, and there was ample time to have hearings to find out about the details of this bill. There was a Judiciary subcommittee hearing on October 1.

The bill was negotiated between the chairman and ranking member and the White House. The Judiciary Committee did not take up the bill. We have had ample time. This bill should have been before the Senate weeks ago. If we had moved on it promptly after it was submitted on the 20th, we could have had hearings, perhaps some in closed session. We could have had a markup. We could have had an understanding of the bill.

When the Senator from Wisconsin has offered two amendments, which I have supported, I am inquiring as to what is the specific concern about law enforcement to preclude the adoption of the amendments of the Senator from Wisconsin and the possible inva- ring-leader and myself and how much longer we are going to be here tonight.

**The PRESIDING OFFICER.** The majority leader.

**Mr. DASCHLE.** Madam President, let me just say, anybody who wishes to speak on this bill is certainly welcome to do so, but we will be here after the vote for anybody who wishes to accom- modate any other Senator who would like to go home.

The hour is late. We have one more amendment, and then we have final passage. It is my hope that we can complete our work on the bill and cer- tainly leave open the opportunity for Senators to express themselves. We will stay just as long as that is re- quired. I hope, though, we can accom- modate other Senators who may not feel the need to participate in further debate.

I yield the floor.

**The PRESIDING OFFICER.** The Senator from Pennsylvania.

**Mr. SPECTER.** Madam President, I had spoken earlier this evening at some length about my concerns as to the procedures on the bill. I want to make a very few brief comments at this time.

I am concerned about the procedures on establishing a record which will withstand constitutional scrutiny. I shall not repeat the citation of the decision of the Supreme Court of the United States which I cited earlier, except to say that the Supreme Court has invalidated acts of Congress where there is not a considered judgment. I understand the position of the majority leader in wanting to get this bill finished. Earlier this evening, I went through an elaborate chronology as to what has happened here. Nine days after September 11, the Attorney General submitted a bill. I had suggested hearings that week. The bill was submitted on September 20. We could have had hearings on September 21 and even on September 22, a Saturday. The Judiciary Committee had one hearing, a very brief one, on September 22. I wrote the chairman of the committee two letters urging hearings, and there was ample time to have hearings to find out about the details of this bill. There was a Judiciary subcommit-tee hearing on October 1.

The bill was negotiated between the chairman and ranking member and the White House. The Judiciary Committee did not take up the bill. We have had ample time. This bill should have been before the Senate weeks ago. If we had moved on it promptly after it was submitted on the 20th, we could have had hearings, perhaps some in closed session. We could have had a markup. We could have had an understanding of the bill.

When the Senator from Wisconsin has offered two amendments, which I have supported, I am inquiring as to what is the specific concern about law enforcement to preclude the adoption of the amendments of the Senator from Wisconsin and the possible inva-
where the Supreme Court of the United States balances law enforcement’s needs with the incursion on privacy.

I feel constrained to make these comments. I hope yet that we can create a record which will withstand constitutional scrutiny.

Again I intend to vote for the bill, but say again that this body ought to be proceeding in a way to establish the record. The worst thing that would happen is if we try terrorists, having used these procedures, and have the convictions invalidated. I have had experiences as a prosecuting attorney and know exactly what that means.

I want my concerns noted for the record. I thank the Chair and yield the floor.

The PRESIDING OFFICER. The Senator from Massachusetts.

Mr. KERRY. Madam President, I have 5 minutes, but I will not use it. I want to make two very quick points.

One, the former prosecutor. I am sympathetic to the comments of the Senator from Pennsylvania. I think all of us ought to be respectful of what the Senator from Wisconsin has been talking about this evening.

I will vote for the bill. I am particularly sensitive to what the majority leader has said about the delicacy and the balance. Even within that delicacy, there are some very legitimate concerns.

It is my hope that when this goes to conference, some of the positions of the Senate will be thought about carefully and respected and that the Senate may even be able to improve what we have by taking those into account.

The second point is that there is within this legislation for the first time a very significant effort on money laundering. I will say to my colleagues that all of the weapons in this war and for all of our might militarily, the most significant efforts to ferret out and stop terrorists are going to come from the combination of information, intelligence that we gather and process, and from our ability to take unconventional steps, particularly those such as the money-laundering measures.

Senator LEVIN has done an outstanding job of helping to frame that, as has Senator SARBANES. The truth is, there are banking interests that even to this moment still resist living up to the standards of the Basel convention and the international standards about knowing your customer and being part of the law enforcement effort rather than a blockade to it.

We are told there may be some effort through the House to try to strip this out. It is my hope that the Senate will stand firm and hold to the full measure of what President Bush has asked us to do.

This will be a long effort, a pains-taking effort. If we are serious about it, we have to have the law enforcement tools to make this happen.

One of the most critical ones is empowering the Secretary of the Treasury to do a reasonable, ratcheted, sort of geared process of addressing the concerns of ferreting out money laundering and taking the money away from these illicit interests around the globe. They are not just in terrorism. They are linked to money laundering. They are all part of the same network which also funds the terrorists themselves.

We recognize that three-quarters of the heroin that reaches the United States comes from Afghanistan. The Taliban and al-Qaeda both trafficking in that heroin. These networks and the interconnectedness of them to the banking institutions, the financial marketplace, are absolutely essential for us as we fight a war on terrorism.

I hope this money-laundering component will be part of the final terrorism bill.

I yield whatever remaining time I have.

The PRESIDING OFFICER. The Senator from Michigan.

Mr. LEVIN. Madam President, I thank Chairman LEAHY, Chairman SARBANES, and members of their committees, for including our very strong anti-money-laundering provisions in the antiterrorism bill.

The antiterrorism bill is simply incomplete unless it has anti-money-laundering provisions. Our provisions are strong provisions. They will help prevent terrorists and other criminals from using our banks to finance their activities in this country to fund their activities which are terrorizing this country.

There apparently is going to be a continuing effort in the House of Representatives to strip the anti-money-laundering provisions, which we have worked so hard on, from the antiterrorism bill. It is my understanding the White House will support keeping those provisions in the bill. Our committees have worked very hard to know that there are no redundant provisions in the antiterrorism bill. Unless these provisions are in there, we are providing the executive branch with only half a tool box in the fight against terrorism.

Three years ago, the minority staff of the Permanent Subcommittee on Investigations which I now chair, began its investigation into money laundering using U.S. banks. Three years, three sets of hearings, two reports and a five-volume record on correspondent banking and money laundering was the result.

We found, not surprisingly, that U.S. banks have accounts for foreign banks and that the customers of those foreign banks can then use the U.S. banks to move their money. But if foreign banks do a poor job in screening their customers, criminals and terrorists can end up using U.S. banks for their criminal purposes.

We found that U.S. banks do a poor job in screening the foreign banks they accept as correspondent customers.

Banks told us “a bank is a bank is a bank” but that’s not true. There are good banks and bad banks. We found numerous banks where the bank was engaged in criminal activity or had such poor banking practices any criminal could be a customer. If a bad bank has a correspondent account with a U.S. bank, customers of that bad bank have access to U.S. financial system. Then criminals, including drug traffickers and terrorists, are able to use our financial systems to carry out their crimes.

In response to what we learned, we developed a bill—S. 1371, the Money Laundering Abatement Act introduced in early August.

It’s a bipartisan bill, and I would like to recognize my cosponsors—in particular, Senator CHUCK GRASSLEY who has helped to lead the fight for including this money laundering legislation on this anti-terrorism bill. The cosponsors in addition to Senator GRASSLEY are: Senators SARBANES, KYL, DEWINE, BILL NELSON, DURBIN, KERRY and SPECTER. The provisions of that bill have been included in the legislation we are now considering.

We now know that the September 11 terrorists used our financial institutions and systems to help accomplish their wish. The terrorists used credit cards, and wire transfers involving U.S. banks in Florida, New York, Pennsylvania. We’ve seen the photos of two of the terrorists using an ATM machine.

Osama bin Laden has bragged about it. There are too many holes that let in bad banks and bad actors, and we need to close them.

Look at what we’ve learned just in the last few days about bin Laden and al-Qaida. Several U.S. banks have had correspondent accounts for a Sudanese bank called the al-Shamil Islamic Bank.

A 1996 State Department fact sheet states that bin Laden helped finance the bank in the amount of $50 million. A respected international newsletter on intelligence matters, Indigo Publications in March 16, 2000, said bin Laden remains a leading shareholder, although the al-Shamil Bank apparently denies that.

The story in the February 2001 criminal trial of the 1998 terrorist bombings of U.S. embassies in Kenya and Tanzania, revealed that a bin Laden associate who handled financial transactions for al-Qaida testified al-Qaida had a half dozen accounts at al-Shamil bank, one of which was in bin Laden’s name. The witness at that trial said in 1994 a bin Laden associate took $100,000—in cash, U.S. Dollars—out of the Shamal Bank paid it to the witness and told him to deliver it to an individual in Jordan, which he did.

Another bin Ladin associate testified at the same trial that he received $250,000 by a wire transfer from the
Shamal Bank to his account in a U.S. bank in Arlington, Texas, to purchase a plane in the United States for bin Laden. He said he personally delivered the plane to bin Laden.

Why did this bank have a correspondent account with the U.S. bank? Why should we allow that to happen?

Even today, when you look at the al Shamal bank website, the bank is still active and advertises an extensive correspondent network. Three U.S. banks have correspondent accounts with this foreign bank. One of these banks has closed its account, but the two other banks continue to have accounts, although the accounts are frozen. Those accounts are now inactive because Sudan, home country of al Shamal, is on the list of terrorist countries and any business with the government of those countries has to be approved. But the accounts were operational at one point in time. Moreover, al Shamal bank has correspondent accounts with other foreign banks which have no connection to the U.S. banks.

That means al Shamal bank can still use the U.S. financial system through an account with a foreign bank that has a correspondent account with a U.S. bank. We call this nesting and it is a problem. It means that al Shamal bank and its customers can still use the U.S. banking system.

The bill before us would require U.S. banks to do a lot more homework on the banks they allow to have correspondent accounts. Under the anti-terrorism bill, it is my belief and my hope that a bank like al Shamal would never be granted a correspondent account at a U.S. bank.

The bill would also allow U.S. law enforcement to capture any illicit funds in a U.S. correspondent account. Now, if a criminal or terrorist has money in a foreign bank that has an account at U.S. bank and illicit money is being held in a U.S. account, law enforcement would find that money unless the person is on the terrorist list or can prove that the foreign bank with the correspondent account is part of a criminal or terrorist act. That’s an excessively hard threshold. This legislation would allow law enforcement to freeze money in correspondent accounts to the same extent they can freeze money in regular, individual accounts.

We need all the tools possible in our arsenal to fight the financial network of terrorism. The money laundering provisions in this bill close the loopholes in existing law and provide additional tools for law enforcement to use. I thank Chairman SARBANES and the other members of the Banking Committee for including so much of the Levin-Grassley anti-money laundering bill, S. 1371, in the Committee’s bill. I also thank Chairman LEAHY and the other Judiciary Committee members for including anti-money laundering provisions of S. 1510, the Terrorism bill. Strengthening our anti-money laundering laws will strike a blow against terrorism by making it harder for terrorists to get the funds they need into United States; an anti-terrorism bill without these anti-money laundering provisions would be providing U.S. law enforcement with only half a toolbox against terrorism.

I would like to take a few minutes to discuss a few key provisions from the Levin-Grassley bill that have been incorporated into S. 1510. These provisions are based on an extensive record of hearings and reports issued in connection with investigations conducted over the past few years by the Permanent Subcommittee on Investigations, which I chair, into money laundering in the correspondent and private banking fields.

The four provisions I want to focus on are provisions that would ban foreign shell banks from the U.S. financial system; require U.S. financial institutions to exercise due diligence; add foreign corruption offenses to the list of U.S. crimes that can trigger money laundering prosecution; and close a major forfeiture loophole involving foreign banks.

First is the shell bank ban in Section 313 of S. 1510. This provision is a very important one, because it attempts to eliminate from the U.S. financial system one category of foreign banks that carry the highest money laundering risks in the banking world today. Those are offshore shell banks, which are defined in the bill, are banks that have no physical presence anywhere and no affiliation with any bank that has a physical presence. Our Subcommittee investigation found that these shell banks carry the highest money laundering risks in the banking world, because they are inherently unavailable for effective oversight. There is no office where a bank regulator or law enforcement official can go to observe bank operations, review documents, talk to bank officials, or freeze funds. In a few countries now issue licenses for unaffiliated shell banks; they include Nauru, Vanuatu, and Montenegro. Nauru alone is believed to maintain licenses for somewhere between 400 and 3,000 offshore shell banks, none of which are being actively supervised, and some of which are suspected of laundering funds for Russian organized crime. A staff report that we issued in February of this year includes four detailed case histories of offshore shell banks to open correspondent accounts at U.S. banks and used them to move funds related to drug trafficking, bribe money and financial fraud money.

The possibility that terrorists are also using shell banks to conduct their operations is clear and cannot be ignored. What is that is why this provision seeks to exclude shell banks from the U.S. financial system. The provision flat-out prohibits U.S. financial institutions from opening an account with a shell bank. This provision would also apply to U.S. financial institutions to take reasonable steps to make sure that other foreign banks are not allowing shell banks to use their U.S. accounts to gain entry to the U.S. financial system. The point is to prevent shell banks from getting direct or indirect access to U.S. financial accounts. The shell bank ban applies to both banks and securities firms operating in the United States, so that it is as broad and as effective as possible.

The provision directs the Treasury Secretary to provide regulatory guidance to U.S. financial institutions on the reasonable steps they have to take to guard against shell banks using accounts opened for other foreign banks. One possible approach would be for U.S. financial institutions to include a new section in the standard language they use to open accounts for foreign banks asking the foreign bank to certify that it will not allow any shell bank to use its U.S. accounts. The U.S. financial institution could then rely on the ground that the requisite certification evidence to the contrary indicating that a shell bank was actually using the account, in which case the financial institution would have to take reasonable steps to determine whether a shell bank was, in fact, using the U.S. account.

The provision contains one exception to the shell bank ban, which should be narrowed significantly to protect the U.S. financial system to the greatest extent possible. This exception allows U.S. financial institutions to open an account for a shell bank that is both affiliated with another bank that maintains a physical presence, subject to supervision by the banking regulator of that affiliated bank. This exception is intended to allow U.S. financial institutions to do business with shell branches of large, established banks on the ground that the established bank can and does observe all of that bank’s branches, including any shell branch.

This exception could, of course, be abused. It is possible that an estab-lished bank in a jurisdiction with weak banking and anti-money laundering controls could open a shell branch in another country with equally weak controls and try to use that shell branch to launder funds in ways that are unlikely to be detected or stopped by the bank regulator in its home jurisdiction. In that case, while the shell bank ban exception would not flat-out bar U.S. financial institutions from opening an account with a shell branch, another provision would come into play and require the U.S. financial institution to exercise enhanced due diligence before opening an account for this shell bank. I would hope that U.S. financial institutions do not open such an account—that they would exercise common sense and restraint and refrain from doing business with a shell operation that is affiliated with a poorly regulated bank and inherently resistant to effective oversight.

Many U.S. financial institutions already have a policy against doing business with shell banks, but at least one
major U.S. bank, Citibank, has a history of taking on shell banks as clients. In order to keep those clients, Citibank tried very hard to expand the exception in this section to also allow U.S. accounts for shell banks affiliated with financially sound foreign banks, such as securities firms or financial holding companies. The broad exception was firmly and explicitly rejected by both the Senate Banking Committee and the House Financial Services Committee, because it would have opened a gaping loophole in the shell bank ban and rendered the ban largely ineffective. All a shell bank would have had to do to evade the ban was establish an affiliated shell corporation and call it a financial services company in order to be eligible to open a U.S. bank account. The Citibank approach would, for example, have allowed a shell bank established by bin Laden's financial holding company, Taba Investments, to open accounts at U.S. securities firms that would have perpetrated the very problem that the Senate investigation identified in two of its shell bank case histories involving M.A. Bank and Federal Bank, each of which opened Citibank accounts to work and underwrite accounts to deposit suspect funds associated with drug trafficking and bribery.

The exception to the shell bank ban is being closely considered, however, and U.S. financial institutions will hopefully use great restraint in doing business with any shell bank that is not affiliated with a well known, well regulated bank. The shell bank ban is intended to close the U.S. financial marketplace to the money laundering risks posed by these banks, and it is my hope that other countries and the Financial Action Task Force on Money Laundering will follow the U.S. lead and take the same action in other jurisdictions.

The next provision is the due diligence requirement in Section 312 of S. 1510. This is another critical provision that tightens up U.S. anti-money laundering controls by requiring U.S. financial institutions to exercise due diligence when opening and managing correspondent and private banking accounts for foreign banks and wealthy foreign individuals.

The provision targets correspondent and private banking accounts, because these two areas have been identified by U.S. bank regulators as high risk areas for money laundering, and because Congressional investigations have documented money laundering abuses through them. For example, two weeks ago, I testified before the Banking Committee about a high risk foreign bank in Sudan that was able to open accounts at major banks around the world, including in the United States and, in 1994, used those accounts to funnel money to bin Laden operations even then living in Texas. On one occasion, he used a $250,000 wire transfer from the Sudanese bank to buy an airplane capable of transporting Stinger missiles, fly it to Sudan and deliver the keys to bin Laden. Six months earlier, we released a staff report with ten case histories of high risk foreign banks that used their U.S. accounts to transact illicit proceeds and to deposit millions of dollars in suspect funds. The bottom line is that U.S. banks need to do a much better job in screening the foreign banks and wealthy foreign individuals they allow to open accounts in the United States.

The due diligence provision would address that problem. It would impose an ongoing, industry-wide legal obligation on all types of financial institutions operating in the United States to exercise greater care when opening accounts for foreign banks and wealthy foreign individuals. Its due diligence requirements are intended to function as preventative measures to stop dubious banks and as well as terrorists or other criminals from using foreign banks' accounts to gain access to the U.S. financial system.

The general obligation to exercise due diligence with respect to all correspondent and private banking accounts is contained in paragraph (1). Paragraphs (2) and (3) then provide minimum standards for the enhanced due diligence that U.S. banks must exercise with respect to certain correspondent and private banking accounts. Paragraph (4)(B) gives the Treasury Secretary discretion to issue regulatory guidance to further clarify the due diligence policies, procedures and controls required by paragraph (1).

The regulatory authority granted in this section is intended to help financial institutions understand what is expected of them. The Secretary may want to issue regulations that help differentiate types of financial institutions to understand their obligations under the due diligence provision. However, one key needs to be made with respect to the Secretary's exercise of this regulatory authority, and that involves how it is to be coordinated with Section 313(a)(6), which authorizes the Attorney General for U.S. courts to make a depositor "subject to a quirk in the law, U.S. law enforcement faces a significant and unusual legal barrier to seizing funds from a correspondent account. Unlike a regular U.S. bank account, it is not possible to apply for a freeze order in court to show that criminal proceeds were deposited into the correspondent account; instead, because funds in a correspondent account are considered to be the funds of the foreign bank itself, the government must also show that the foreign bank was somehow part of the wrongdoing.

That's not only a tough job, that can be an impossible job. In many cases, the foreign bank will not have been part of the wrongdoing, but that's a strange reason for letting the foreign depositor who was engaged in a wrongdoing escape forfeiture. And in those cases where the foreign bank may have
been involved, no prosecutor will be able to allege it in a complaint without first getting the resources needed to chase the foreign bank abroad. Take, for example, the case of Barclays Bank which has frozen an account suspected of being associated with terrorism. If that account had been a correspondent account in the United States opened for Barclays Bank, U.S. law enforcement could have been unable to freeze the particular deposits suspected of being associated with terrorism, because the funds were in the Barclays correspondent account and Barclays itself was apparently unaware of any wrongdoing. That doesn’t make sense. U.S. law enforcement should be able to freeze the funds.

Section 319(a) would eliminate that quirk by placing civil forfeitures of funds in correspondent accounts on the same footing as forfeitures of funds in all other U.S. accounts. There is just no reason banks should be shielded from forfeitures when U.S. banks would not be.

Section 319 has many other important provisions as well, including provisions dealing with Federal Receivers, legal service on foreign banks and more. I want to again thank Senator Sarbanes and Senator Leahy and their staffs for their hard work and cooperative spirit in bringing this bill to the floor and including the provisions of our bill in it.

I need to add that the hard work in passing this bill will be for naught if some of the banks have their way in the House and in Committee. I’m very concerned with reports that there is an effort in the House to separate the money laundering and anti-terrorism bills, so money laundering will be considered separately. The banks should be working with us to ensure all the problems highlighted in the Attorney General’s speech—the need to add to the list of foreign offenses that constitute predicate crimes for money laundering prosecutions—is included in the final bill. The bipartisan provisions in your bill would greatly improve our money laundering laws.

As the Attorney General also indicated in his speech, the Department of Justice has been developing its own proposal to update our money laundering laws and we hope to provide Congress with our own recommendations in the near future. We look forward to working with you in pursuing our mutual goal of strengthening and modernizing our money laundering laws to meet the challenges of this new century.

Thank you for your attention to this matter. If we may be of additional assistance, we look forward to working with you to ensure that your efforts to combat money laundering and terrorist financing are not undercut by the efforts of foreign banks from around the world to evade U.S. laws. U.S. law enforcement should be able to freeze the funds.

Sincerely,

DONALD E. POWELL, Director.

Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for the opportunity to comment on S. 1371, the Money Laundering Abatement Act. The Federal Deposit Insurance Corporation is concerned about the damage to the U.S. financial system that may result from money laundering activities and we congratulate you for your leadership in this area.

As deposit insurer, the FDIC is vitally interested in preventing insured depository institutions from being used as conduits for funds derived from illegal activity. As you may know, in January of this year, the FDIC, along with the Department of the Treasury, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Department of State, issued Guidance On Enhanced Scrutiny For Transactions That May Involve The Proceeds Of Official Corruption. The FDIC is also an active participant in other working groups that seek more effective ways to combat money laundering.

Chairman, Senate Drug Caucus, U.S. Senate, Washington, DC.

S. 1371 is an important step in trying to prevent foreign entities from laundering money through U.S. financial institutions. S. 1371 would, in several ways, require U.S. financial institutions to identify foreign parties who open or maintain accounts with U.S. financial institutions, such as correspondent accounts or private banking accounts. The bill would also prohibit customers from having direct access to concentration accounts, and make it a crime to falsify the identity of a participant in a transaction outside the U.S. or through U.S. financial institutions. Correspondent and concentration accounts have the potential to be misused so as to facilitate money laundering, and the bill appropriately addresses these concerns.

One point we would like to raise is in relation to Section 3 of the bill. Section 3 provides for consultation between the Board of Governors of the Federal Reserve System and the Secretary of the Treasury, both in regard to devising measures to combat money laundering and defining terms relating to anti-money laundering measures. The FDIC believes that such consultation requirements should include the FDIC as well as the other Federal banking agencies.

Chairman.

October 11, 2001

Hon. Carl Levin, Chairman, Senate Drug Caucus, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for your efforts to combat money laundering and terrorist financing. We greatly appreciate your initiative in this important area and believe that several provisions of S. 1371 would be of particular benefit to DEA’s efforts to combat money laundering. As Acting Assistant Attorney General, Mr. Bryant recently indicated in his letter to you, the Administration has been working for some time on a package of additional suggested money laundering amendments, which we hope to be able to share with you shortly.

We look forward to working with you to strengthen and improve the Nation’s money laundering laws. If I can be of any further assistance, please do not hesitate to contact me. The Office of Management and Budget has advised that there is no objection to the presentation of this report from the standpoint of the Administration’s program.

Sincerely,

DONALD E. POWELL, Chairman.
The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. Madam President, I tell the distinguished Senator from Michigan and the distinguished Senator from Massachusetts, who made such strong and valid points on money laundering, we just received from the administration their statement of policy saying: This includes money laundering, other financial infrastructure provisions arising from bank legal legislative proposals. These provisions were added to this bill after unanimous approval to have these provisions in the Senate Banking Committee. The administration supports the effort to strengthen this.

And so on. They are extremely important, and I can assure both Senators that I will strongly support retention of this in conference.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Mr. President, I call up amendment No. 1901, which is at the desk.

The PRESIDING OFFICER (Mr. MILLS). The clerk will report.

The legislative clerk read as follows:

The Senator from Wisconsin [Mr. FEINGOLD] proposes an amendment numbered 1901.

Mr. FEINGOLD. I seek unanimous consent that further reading of the amendment be dispensed with.

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

The amendment is as follows:

(Purpose: To modify the provisions relating to access to business records under the Foreign Intelligence Surveillance Act of 1978)

Strike section 215 and insert the following:

SEC. 215. ACCESS TO BUSINESS RECORD UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(A) In general.—Section 502 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1862) is amended—

(1) in subsection (a), by striking "authorizing a common carrier" and all that follows through "and related purposes" and inserting "requiring a business to produce any tangible things (including books, records, papers, documents, and other items);"

(2) in subsection (b), by striking "and" at the end; and

(3) by adding at the end the following new subparagraph:

"(C) the records concerned are not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes;"

(b) CONFORMING AMENDMENT.—The text of section 501 of that Act (50 U.S.C. 1801) is amended to read as follows:

"Foreign intelligence; the FBI cannot go on a business has concentration of money laundering. My colleagues in the U.S. Justice Department indicate that this and similar laws are essential if we are to succeed in our fight against organized crime, drug dealers, and terrorism. This bill is the result of lengthy hearings and congressional fact-finding that concluded that the regulations set forth in the bill are needed. The bill has my support, and I would urge its passage as soon as possible.

Sincerely yours,

JENNIFER M. GRANHOLM, Attorney General.

STATE OF MICHIGAN,
OFFICE OF THE ATTORNEY GENERAL,

HON. CARL LEVIN,
U.S. Senator, Senate Russell Senate Office Bldg.,
Washington, DC.

Dear Senator LEVIN and GRASSLEY: I write to express my strong support for S1371, the Money Laundering Abatement Act. This is a problem that has allowed the criminal element to secrete the proceeds of criminal activity and to generate funds needed to facilitate and underwrite organized crime.

The bill will make it harder for foreign criminals to use United States banks to launder the proceeds of their illegal activity and to allow investigators to detect, prevent, and prosecute money laundering. In particular, the bill strengthens existing anti-money laundering laws by adding foreign corruption offenses, barring U.S. banks from providing banking services to foreign shell banks, requiring U.S. banks to conduct enhanced due diligence and making foreign bank depositors' funds in U.S. correspondence banks subject to the same forfeiture rules that apply to funds in other U.S. bank accounts.

Recent events highlighting the activities of foreign terrorists have demonstrated the necessity of this legislation. My colleagues in the House of Representatives and in the Senate Judiciary Committee and in foreign bank accounts.

Your bill is an example of the immense value of the information provided by the Permanent Subcommittee on Investigations, because this type of bill requires a deeper understanding of the issues that comes from long term inquiries by professional staff. We who are involved in state level money laundering control efforts should be particularly supportive of such long term strategies because they are more important to the quality of life of our citizens.

I commend your efforts for introducing this important legislation and will assist you in any way I can to gain its passage.

Yours very truly,

JANET NAPOLITANO,
Attorney General.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Mr. President, I call up amendment No. 1901, which is at the desk.

The PRESIDING OFFICER (Mr. MILLS). The clerk will report.

The legislative clerk read as follows:

The Senator from Wisconsin [Mr. FEINGOLD] proposes an amendment numbered 1901.

Mr. FEINGOLD. I seek unanimous consent that further reading of the amendment be dispensed with.

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

The amendment is as follows:

(Purpose: To modify the provisions relating to access to business records under the Foreign Intelligence Surveillance Act of 1978)

Strike section 215 and insert the following:

SEC. 215. ACCESS TO BUSINESS RECORD UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(A) IN GENERAL.—Section 502 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1862) is amended—

(1) in subsection (a), by striking "authorizing a common carrier" and all that follows through "and related purposes" and inserting "requiring a business to produce any tangible things (including books, records, papers, documents, and other items);"

(2) in subsection (b), by striking "and" at the end; and

(3) by adding at the end the following new subparagraph:

"(C) the records concerned are not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes;"

(b) CONFORMING AMENDMENT.—The text of section 501 of that Act (50 U.S.C. 1801) is amended to read as follows:

"SEC. 501. In this title, the terms 'agent of a foreign power', 'foreign intelligence information', and 'international terrorism' mean the same things as those terms mean in section 101."

Mr. FEINGOLD. Mr. President, this amendment has to do with section 215 in the bill. It allows the Government, under FISA, to compel businesses to turn over records to assist in an investigation of terrorism or espionage. The provision makes two significant changes from current law. Under current law, the FBI can seek records from public accommodations, such as hotels and motels, car rental companies, storage facilities, and travel records, such as those from airlines.

Current law also requires the FBI to demonstrate to the State Court that the records pertain to an agent of a foreign power. The FBI cannot go on a fishing expedition of records of citizens of this country who might have had incidental contact with a target of an investigation. But under section 215 of this bill, all business records can be compelled to be produced, including those containing sensitive personal information such as medical records.
from hospitals or doctors, or educational records, or records of what books someone has taken out of the library. This is an enormous expansion of authority, compounded by the elimination of any requirement that the records have to pertain to an agent of a foreign power. Under this provision, the Government can apparently go on a fishing expedition and collect information on anyone—perhaps someone who has worked with, or lived next door to, or has competed in the company of, or went to school with, or whose phone number was called by the target of an investigation.

So we are not talking here only about the targets of the investigation; we are talking about people who have simply had some incidental contact with the target. All the FBI has to do is to allege in order to get the order that the information is sought for an investigation of international terrorism or clandestine intelligence gathering. That is all they have to do, assert that—not to just get at the targets, but at people who have had any contact whatsoever with them.

On that minimal showing in an ex parte application to a secret court, the Government can lawfully compel a doctor or a hospital to release medical records or a library to release circulation records. This is truly a breathtaking expansion of the police power, one that I do not think is warranted.

My amendment does not completely strike the provision. There are elements of it that I think have legitimacy. First, my amendment maintains the requirement that the records pertain to a target alleged to be an agent of a foreign power. This provides some protection for American citizens who might otherwise become the subject of investigations for having some innocent contact with a suspected terrorist.

Second, while the amendment maintains the expansion of the FISA authority to all business records, it also requires the FBI to comply with State and Federal laws that contain a higher level of privacy protection. The amendment makes it clear that existing Federal and State statutory protections for the privacy of certain information are not diminished or superseded by section 215.

There are certain categories of records, such as medical records or educational records, that Congress and State legislatures have deemed worthy of a higher level of privacy protection. Let me quickly give you a couple of examples. In California, there is a very detailed statutory provision governing disclosure of medical information to law enforcement authorities. Generally, the law requires either patient consent, or a court order, or a subpoena issued on an order of the court, to produce the record. The court must, among other things, find good cause based on a determination that there is a reasonable likelihood that the records in question will disclose material information or evidence of substantial value in connection with the investigation or prosecution.

Montana is another State with strong statutory or constitutional, protections for medical records. It provides that medical records can only be obtained with an investigative subpoena signed by a judge, and that such subpoena may be issued only when it appears upon the affidavit of the prosecutor or other law enforcement officer of the interest requires it to be issued. In order to establish a compelling State interest, the prosecutor must state facts and circumstances sufficient to support probable cause to believe that an offense has been committed, and that the information relative to the commission of that offense is in the possession of the person or institution to whom the subpoena is directed.

My State of Wisconsin, along with many other States, has strong library confidentiality laws which require a court order for disclosure of public library system records.

"Texas, for example, permits disclosure of library records "to a law enforcement agency or prosecutor under a court order or subpoena obtained after a showing to a court that: (A) disclosure of the record is necessary to protect the public safety; (B) the record is evidence of an offense or constitutes evidence that a particular person committed an offense." Missouri and Nevada library records confidentiality laws both require that a court find "that the disclosure of such record is necessary to protect the public safety or to prosecute a crime."

South Carolina’s library records confidentiality law permits disclosure "in accordance with a proper judicial order upon finding that disclosure of the records is necessary to protect public safety, to prosecute a crime, or upon showing of good cause before a presiding judge in a civil matter."

In short, our States have made policy judgments about the protection to which certain kinds of records are justified. We have Federal laws that express similar judgments—Federal Educational Records Privacy Act. Indeed, as I will mention, this bill provides new standards for the production of educational records in connection with terrorism investigations. So may fear that Section 215 as written may be interpreted to require that the protections I seek to preserve with scant discussion of either the merits or the consequences of such a proposal, during a time of incredible strain on our democratic principles, and for an indeterminate length of time.

If my amendment is adopted, law enforcement will still have access to all of the information it seeks. But my amendment simply maintains the integrity of protections enacted by Congress and State legislatures for certain kinds of sensitive information to ensure that access to this information is given only where it is necessary. It makes sure that this provision does not become the platform or an excuse for a fishing expedition for damaging information on American citizens who are not the subjects of FISA surveillance.

I reserve the remainder of my time.

The PRESIDING OFFICER. The Senator from Minnesota is recognized.

Mr. FEINGOLD. I yield 5 minutes to the Senator.

Mr. WELLSTONE. Mr. President, I say, again, to colleagues that this amendment the Senator from Wisconsin introduced makes sure that our proposed an order of a FISA court does not apply for an order of a FISA court does not apply if another State or Federal law governs the law enforcement or intelligence access to the record.

To the extent that the records sought have no such statutory protection, the only effect this amendment would have is to ensure that the records actually pertain to the target. But I strongly believe that merely alleging that the records are needed for an intelligence investigation should not override other protections provided by State and Federal law.

I will quickly highlight the problem by referring to section 508 of this bill. That section, I think, would be rendered meaningless if section 215 is not amended as I propose.

The original version of section 508 proposed by the administration would have given the Attorney General the right to obtain the educational records of virtually any student without a court order. I and many other Senators had serious problems with that provision, and it was significantly changed before S. 1510 was introduced. Section 508 now does require a court order and does provide a specific showing that the Attorney General must make to obtain the order to get at these educational records. But if section 215 is enacted without my amendment a university could be ordered to turn over such records as "tangible things" on a much lower showing.

The administration asserts that it is too great a burden for the Government to abide by existing privacy protections and seek court orders to obtain certain sensitive information specifically identified by Congress and State legislatures. I remind my colleagues that the protections I seek to preserve were carefully drafted and debated and enacted at a time when legislators could thoughtfully consider the full weight of granting such protections. We are now asked to set these protections aside with scant discussion of either the merits or the consequences of such a proposal, during a time of incredible strain on our democratic principles, and for an indeterminate length of time.
The amendment of the Senator from Wisconsin goes to the heart of the concern that a lot of the people we represent have. I imagine that the vote may be overwhelmingly in opposition to this amendment. That has been the pattern.

Again, I thank the Senator from Wisconsin for raising these questions. This is what we should be doing.

I conclude this way: I really think, in part, because of the kind of questions the Senator from Wisconsin has raised—again, I am not a lawyer—in looking at this bill, Mr. President, I say to Senator LEAHY, it seems to me he and others have done a great job and are doing everything possible to make this more balanced. There are so many good provisions in this bill that we need, I believe that.

I hope we can keep the sunset provision, which is so essential to oversight, because I think what is good is the provisions of this legislation that focus on combination and realism and what is not quite so good is the parts of this bill that reach way beyond that.

Yes, there is a lot of good. I will support it. I will reserve final judgment of what comes out of the conference committee. We can make it better.

I thank my colleagues, Senator HATCH included, for their work. Sometimes people can honestly disagree. I know this is important. I know where we are as a nation, but the Senator from Wisconsin has raised important concerns tonight, and as well as we hope we do better in conference. I yield the floor.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Mr. President, I thank the Senator from Minnesota. He said it exactly right. Each of us who spoke on these amendments tonight cares just as much as everybody in this room about the fight against terrorism and some just want to make sure we do not go beyond that goal with unnecessary language that intrudes on our civil liberties. That is it. That is all we are trying to do.

I am pleased to yield 5 minutes to the Senator from Washington.

The PRESIDING OFFICER. The Senator from Wisconsin.

Ms. CANTWELL. Mr. President, I thank the Senator from Wisconsin for the time and his energies this evening. We are a country that has raised important concerns and we have a lot of work to do. We are a country that has raised important concerns tonight, and as well as we hope we do better in conference.

I am very proud of the many tools in the bill for law enforcement. I ask unanimous consent that the column in the Washington Post be printed in the RECORD.

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

[From the Washington Post, Oct. 10, 2001]

When Care Beats Haste

The complex and ambivalent legislation that the administration sent Congress less than a month ago could reach the floors of both houses this week. The original proposal has been gutted by the Senate. And while any submission, but civil liberties groups continue to warn with cause that some of the detention and surveillance provisions would give the government powers that are either necessary or healthy.

Some of the members of both parties who helped construct the current compromises are likewise uneasy about their own handiwork, but reluctant to see as holding up a bill the administration insists it needs right away. The reluctance will be the greater now that the country is engaged in military action in Afghanistan; there is fear—we have no doubt well-founded—of retaliation. But dangerous moments are precisely the ones when it is most important that civil liberties be protected.

The House Judiciary Committee has dealt with the conflicting pressures in part by putting on the table a kind of the surveillance sections of the bill. It has "sunset" them, meaning the powers they confer will expire after two years unless a subsequent Congress, having had two years to work out, votes to extend them. The administration opposes the sunset provision and succeeded in keeping it out of the Senate version. But it's a reasonable compromise. A bill such as this is a balancing of risks—the risk of further attack versus the risk to civil liberties in seeking to forestall the attack. If the bill is as benign as the administration insists, it has nothing to fear from a sunset provision, which ought to be retained.

Parts of the administration proposal were sensible and are not in dispute: allowing the government in an age of cell phones to seek court approval for placing a wiretap on a particular phone, for example. Others were drawn too loosely, and some still need work. The administration had sought authority to detain indefinitely non-citizens, a general power that has been retained. A person not charged with a crime after seven days can be held only if the government is moving to deport him. The question, which the bills don't clearly answer, is how has judicial determination, can it hold him then?

Wiretap authority now is easier to get for foreign intelligence than for law enforcement purposes. The legislation would make it easier still. The question then becomes how to make sure that the new authority isn't abused—indeed used for law enforcement purposes or fishing expeditions—in such a way as to make such surveillance far more commonplace than now. Related issues have to do with the sharing of law enforcement information among government officials. There are ways to provide the broader authority the government says it needs while hedging against its abuse; in our view, not all of those have been fully explored.

So too with the power the bill would give law enforcement officials to obtain records and other things, including e-mail addresses of e-mail sent and received. Phone records are now available to law enforce-
ment agencies more or less on request—when were calls made from phone A to phone B? what should be the Internet analogy?

The administration was said yesterday to be pressing for quick passage by both houses of the Senate measure; the more careful work of the House Judiciary Committee would be set aside. That's wrong, and an acquiescent step that in the long run Congress likely would regret.

Ms. CANTWELL. This article said it best with the headline: "When Care Beats Haste":

Later it says that it would be wrong for us to take an acquiescent step that in the long run would really hurt our country.

What Senator FEINGOLD is simply trying to say is that we have already painstakingly over many years crafted our laws to protect personal privacy. This language in section 215 changes that. It basically says that the FBI can have access to other things, including business records from U.S. citizens who may have had incidental contact with someone who is defined as a terrorist.

Think about that for a second. If you are an employer and someone in your company has now been accused of these things, then under investigation, your business records can also be attained if, as Senator FEINGOLD said, it was deemed part of this investigation, with very minimal judicial review.

Take for another example, you happen to live across the hall from someone who now has become a suspect. Maybe you have been over to their house for dinner several times. Now, all of a sudden, you may be part of that investigation, and your financial records, your medical records, your personal records can now be part of that investigation, again, with very minimal judicial review.

I have examples from many in my State, including my State librarian, consumers, and businesses that are concerned, that this provision is far too broad.

It takes little imagination, as I said, to think of all the tangible items this would give the FBI carte blanche to examine some people's most private and personal papers.

The bottom line is this legislation could circumvent or supersede Federal and State privacy laws that protect student records, library records, and health records not previously admissible under FISA.

What we are talking about in the Feingold amendment is trying to prevent the Senate from approving a law that already specify protection. The amendment simply states where Congress or a State legislature has enacted a law which requires an order to obtain records, that Federal or State law stands.

That seems pretty simple. We have not worked on these issues. We should not work on them in haste.
Mr. LEAHY. Mr. President, the Senator from Vermont wanted to say something for the record.

Mr. HATCH. Mr. President, I thank my colleagues.

I oppose Senator FEINGOLD’s amendment to Section 215 of the bill. Section 215 allows federal law enforcement to apply for a court order to obtain records and other evidence in the course of an investigation to protect against terrorism or clandestine intelligence activities. This provision has many safeguards built in to prevent its misuse.

For instance, the application must be made by the Director of the FBI or his designee, whose rank cannot be lower than an Assistant Special Agent in Charge, and specify that the records concerned are sought for an authorized purpose. This bill cannot be weaker than an Assistant Special Agent in Charge, and specify that the records concerned are sought for an authorized investigation to protect against international terrorism or clandestine intelligence activities. Additionally, the investigation must be conducted pursuant to approved Attorney General guidelines and may not be conducted on a United States person solely upon the basis of activities protected by the first amendment to the Constitution.

As written, the provision balances the investigatory needs of the FBI with privacy concerns and provides adequate protection, while not allowing a host of state-law provisions to stand in the way of national security needs. Senator FEINGOLD’s amendment would condition the issuance of the court order on a myriad of federal and state-law provisions. Such conditioning will have the effect of making investigations to protect against international terrorism more difficult than investigations of certain domestic criminal violations.

Senator FEINGOLD’s amendment purports to preserve privacy protections in place for certain records. The amendment’s effect, however, will be to place foreign intelligence and intelligence investigations at a disadvantage to criminal investigations. For example, this amendment would make it more difficult for the government to obtain business records in a foreign-intelligence or foreign-counter-intelligence invention through a court order than it is to obtain the same records in a criminal health-care fraud or child pornography investigation through a grand jury subpoena or administrative subpoena. (see 18 U.S.C. 3486).

Federal law enforcement officials investigating the activities of a terrorist organization or foreign intelligence target should not face a greater burden than that imposed on investigators of health-care fraud or child pornography.

I urge my colleagues to vote against this amendment.

Mr. LEAHY. Madam President, the administration originally wanted administrative subpoena authority in foreign intelligence cases for government access to any business record. I was able to reach agreement with the administration to subject this authority to judicial review and to bar investigations based on the basis of activities protected by the First Amendment.

The Feingold amendment would ensure that current laws providing safeguards for certain types of records, such as medical and educational records, be maintained. Again, it is unfortunate that the administration did not accept this amendment.

Mr. President, we are prepared to yield back the remainder of our time if the Senator from Wisconsin is prepared to yield back the remainder of his time.

Mr. FEINGOLD. If the majority leader is going to speak, I would like to respond. If not, I will simply yield back the remainder of my time.

Mr. LEAHY. I yield back the remainder of our time.

Mr. DASCHLE. Mr. President, I move to table the amendment and ask for the yeas and nays.

The PRESIDING OFFICER. The question is on agreeing to the table the amendment and ask for the yeas and nays.

Mr. STEVENS. Mr. President, I move to offer an amendment to insure that Northern Border Security. This bill will triple the number of Border Patrol, Customs Service, and INS inspectors along America’s northern borders. It also authorizes $100 million to improve INS and Customs technology and for additional equipment for monitoring the northern borders. Alaska and Alaskans are in a unique position. One section of our northern boarder stretches from Maine through, my good friend’s home state of Vermont, all the way to Washington State. A second section is that of my home State. As you know we are the largest State in the Nation with an enormous border with Canada that runs over 1,538 miles. We have one of the busiest international cargo airports in the world, which has lost a number of carriers since the September 11 attacks due to grossly inadequate staffing at our secure, sterile customs facility. We also have several major international ports scattered throughout Alaska including the Port of Anchorage, which handles the container traffic in Alaska; Dutch Harbor, which is America’s busiest commercial fishing port; and Valdez, where millions of barrels of North Slope crude oil are sent by pipeline to the “South 48.”

The amendment is an addition to the bill that addresses Northern Border Security. This amendment is a vote of confidence in the Senate.

The amendment is a vote of confidence in the Senate.

The amendment is a vote of confidence in the Senate.

The amendment is a vote of confidence in the Senate.

The amendment is a vote of confidence in the Senate.
Mr. SMITH of New Hampshire. Mr. President, I would say to my colleagues, all the tools we are giving to the Department of Justice in this bill are irrelevant if we cannot deport these terrorist who are living in our country. Preparing to terrorize American citizens. Page 162 of the bill says the Attorney General shall place an alien in detention for 7 days of catching him, or charge him with a criminal act, or else the bill says “the Attorney General shall release the alien.” Mr. President, the problem is that most of these terrorist have not committed criminal acts until they are ready to attack. Therefore, in most of these cases, the only option is to deport them.

Mr. LOTT. It is my opinion, that if we cannot deport known terrorist, we should do it. We cannot let the Justice Department be barred because the evidence was too sensitive to use in Court. Mr. SMITH of New Hampshire. That is exactly the problem. Under current laws, we would have to give a declassified summary of all the secret evidence used in the deportation proceedings to the terrorist. Now, why would we compromise our intelligence sources and methods by revealing sensitive information to a known terrorist? The intelligence community would never allow it, and with good reason. But as a result, the Justice Department has never once used the alien terrorist removal court to deport anyone.

Mr. LOTT. That is my understanding, and it is a serious problem. I am in complete agreement with the Senator.

Mr. SMITH of New Hampshire. Mr. President, I am going to support this legislation. As I said, it had been my intention to offer an amendment to resolve this problem by eliminating the requirement for the Attorney General to give this sensitive information to the alien terrorist before deportation. After discussion with the Attorney General, who indicated to me that he supports this provision, and after discussions with the Leader, I have decided in the interest of removing this legislative obstacle to withhold my amendment at this time, with the assurance of the Leader and the Administration that we will work to solve this problem in conference.

Mr. LOTT. Let me say to the Senator that he can count me as a cosponsor of this amendment. It is an excellent amendment, it is needed, and I commit to the Senator that I will do my best to see that it is added in conference. I have also talked about this issue with the Attorney General, and he indicated to me that the Administration supports your amendment and that he will also work to support it in conference. So I appreciate his withholding at this time so we can get this bill to conference where we can work to get the Smith amendment added to greatly improve this bill.

Mr. SMITH of New Hampshire. I thank the Leader for his strong support, and I am pleased that the administration is also supportive. I know how many long hours the Attorney General is put by in this issue, and how committed he is to winning this war on terrorism. I look forward to passing this important provision which will be an invaluable tool for the Attorney General and the President in this war.

DEFFERING MONEY LAUNDERING

Mr. SCHUMER. Mr. President, I would like to clarify with Chairman SARBRANES my understanding of the provision in Title III, the anti-money laundering provisions in the antiterrorism package, entitled “Section 314. Cooperative Efforts to Deter Money Laundering”.

As the Chairman is well aware, Section 314(b) is intended to address concerns about regulatory barriers that stand in the way of developing efficient mechanisms and services that financial institutions can use to fulfill their regulatory compliance obligations. The regulations to be issued by the Treasury and potentially by bank and thrift regulators as well, could further this purpose by reconciling rules that could be interpreted in a way that places conflicting burdens on financial institutions.

Does that comport with the Chairman’s understanding of the intent of the provision and how that intent could best be carried out by the regulators?

Mr. SARBRANES. I thank the Senator for his question. Yes, that is also my understanding of Section 314.

Mr. CORZINE. Mr. President, I am going to support this legislation, and I am going to support it with the Leaders—Senators DASCHLE and LOTT—and Senators LEAHY and HATCH, for their efforts in developing the bill. Clearly, there is no higher priority than combating terrorism and protecting our national security at the same time. We have real concerns about the process by which this legislation has come to the floor, and about the implications of some provisions for fundamental civil liberties.

There are several provisions in this legislation that make a real, positive contribution to the fight against terrorism. Other senators have discussed
some of the highlights in more depth, so let me just focus on a few.

First, this bill includes legislation approved by the Senate Committee on Banking, Housing, and Urban Affairs, on which I sit, that will help authorities combat money laundering. This is essential if we are to deprive terrorists of resources. The bill will require additional reporting of suspicious transactions, require identification of the foreign owners of certain U.S. accounts, and other requirements on financial institutions to give authorities a greater ability to identify and prosecute money launderers. I also note that the bill includes a provision I authored that calls for a study into the possibility of expanding the legislation to include hedge funds and other investment services that also can be used by terrorists to launder money.

Beyond the money laundering provisions, I also am pleased that this bill provides additional funding for the Victims of Terrorism Fund. Coming from New Jersey, where thousands of our residents have been victimized by the tragedy at the World Trade Center, this is especially important to me. In my view, we as a nation have a responsibility to ensure that terrorism victims and their families are not left alone and uncompensated. That is why I am pleased that the bill would replenish the antiterrorism emergency reserve, replace the annual cap on the Crime Victims’ Compensation fund, and strengthen services for victims in other ways. While this is not all that we should be doing for victims and their families, I appreciate the work of the leaders in focusing on their needs.

I also pleased that the bill would triple the number of Border Patrol, Customs Service and immigration inspectors at our northern border. This would significantly enhance security over an area that has seemed understaffed. The bill also authorizes $100 million to improve INS and Customs technology and additional equipment for monitoring the U.S.-Canada border.

In addition, I want to highlight language in this bill that would establish new crimes related to bioterrorism, including provisions to prohibit certain people from possessing a listed biological agent or toxin. There are many reasons we need to prepare for the threat of a biological or chemical attack, and I have introduced related legislation, S. 1508, that would require states to develop coordinated plans, and that would provide additional resources for hospitals and other health care providers. The threat of bioterrorism is real, and I would hope that our leaders will bring related legislation to the Senate floor as soon as possible.

While I support the provisions in this bill on money laundering, victim services, border enforcement, and bioterrorism, I do have serious concerns about the way this bill was put together, and about other provisions that raise serious questions about the protection of civil liberties.

It is deeply troubling to me that we would be taking up a bill that deals with such sensitive civil liberties matters on a rush basis, and without even consideration by the relevant committee. We are talking about a 243-page bill that was developed behind closed doors by a handful of people operating under enormous time pressure. This raises fundamental questions that go to the very essence of our democracy, and our freedoms. It’s not something that should be done in haste, with so little opportunity for input from outside experts, the public, and all senators.

Perhaps because the legislation was developed so quickly, and in an environment so dominated by great public anxiety about security, there is a real risk that we will make serious mistakes. I am especially concerned about the provisions in this bill that require the detention of immigrants who are not terrorists, who are not criminals, but are merely suspected of future wrongdoing. In fact, these provisions go further still—providing that residents who are charged with being deportable on terrorism grounds could be held indefinitely even if an immigration judge determines that the terrorist charges are false. I want to make clear that we need to give the government sufficient authority to protect Americans from those who pose a real threat to public safety. But this provision goes too far. And I hope it can be corrected in conference.

Similarly, there are other provisions of this legislation that seem very loosely drafted, and that could, perhaps unintentionally, lead to infringement on important civil liberties. For example, many have raised serious questions about the law enforcement surveillance of Internet and telephone use, and about other provisions that give the government extensive new powers to conduct secret searches. These and other provisions do not seem to have received adequate scrutiny. I am hopeful that they can be examined more closely in conference, and any needed improvements can be made before the legislation is sent to the President.

I also urge our conferees to accept a provision, like one included in the House version of this legislation, that would set a time limit on the application of certain provisions that pose the greatest threats to civil liberties. In my view, that’s especially important since we have rushed this legislation through the Senate so quickly. As I said, I am hopeful that we can identify and correct any mistakes in conference. But we still seem to be operating on a rush basis, and I suspect that it is inevitable. Given the stakes involved, I think it would be better to make many of these provisions temporary, and then revisit these issues when we have more time to thoroughly consider all their implications.

In the end, while I do have serious concerns about certain aspects of this legislation, I have decided to support the effort to move it to conference. Our nation has just suffered the most horrendous act of terrorism in our history, and we are facing serious threats of other terrorist attacks. A vast, well-organized and well-funded terrorist network has gone to war against our nation, and while we should not over-react, or erode basic freedoms, we do have to defend ourselves.

We must give our law enforcement officials the tools they need to find and destroy these terrorist networks. And this legislation should help. But we need to continue to review and improve its provision as we go to conference. And we will need to continue to closely review the implementation of the legislation after it is enacted.

I yield the floor to Ms. Cantwell. Mr. President, I support this bill, but I do so only with some reservations.

We are giving broad new powers to our law enforcement and intelligence agencies—without additional safeguards of judicial review and congressional oversight.

I believe that many provisions of the bill, particularly those sections dealing with electronic eavesdropping and wiretapping, are seriously flawed and may infringe on civil liberties.

I am voting for this bill today with the strong hope that it will be improved in a conference with the House. As it currently stands, the Senate bill breaks down the traditional separation of domestic criminal matters governed by the fourth amendment right against unjustified search and seizure—from the gathering of international intelligence information traditionally gathered without the same concern for constitutional rights.

I strongly believe that we should have included in this bill a sunset provision that would give Congress the opportunity to reassess whether these new tools are yielding the intended results in the war on terror, and I am hopeful that the final bill will emerge with this and other improvements.

If this bill is not improved through a conference process or other negotiation, I reserve the right to vote against a conference report.

However, I also believe this bill contains many provisions that will significantly advance our battle against terrorism. I thank the Chairman for his hard work on these provisions and appreciate his efforts particularly to strengthen security on our northern border.

Among the most important provisions in this bill is the authorization to triple staffing across our northern border.

These increases in manpower are desperately needed. The northern border is
Mr. EDWARDS. Mr. President, I rise in support of S. 1510, the Uniting and Strengthening America Act.

In the aftermath of September 11, we face two difficult and delicate tasks: to strengthen our security in order to prevent future terrorist attacks, and at the same time, to safeguard the individual liberties that make America a beacon of freedom to all the world.

I believe that when the President signs this anti-terrorism legislation into law, we will have achieved those two goals as best we now can.

The act is a far-reaching bill. I will mention just a few key aspects of that bill.

First, the legislation brings our surveillance laws into the 21st century. Here are two of many examples. Under current law, the FBI needs a basic search warrant to access answering machine messages, but the FISA needs a different kind of warrant to get to voice mail. This law says the FBI can use a traditional warrant for both.

Another example: Under current law, a Federal court can authorize many electronic surveillance warrants only within the court's limited jurisdiction. If the target of the investigation is in the judge's jurisdiction, but the subject of the warrant is an Internet service provider located elsewhere, the warrant is no good as to that ISP. This bill allows the court overseeing an investigation to issue valid warrants nationwide.

Second, the act gives law enforcement officers and the foreign intelligence community the ability to share intelligence information with each other in defined contexts. For example, if they are not under special conditions, the FBI may share wiretap and grand jury information related to foreign and counter-intelligence. I appreciate concerns that this information-sharing authority could be abused. Like Chairman LEAHY, I would have preferred to see greater judicial oversight of these data exchanges. But I also believe we simply cannot prevail in the battle against terrorism if the right hand of our government has no idea what the left hand is doing.

Third, the act enhances intelligence authorities under the Foreign Intelligence Surveillance Act (FISA). When I met with FBI agents in North Carolina shortly after September 11, they told me their number one priority was to streamline the FISA process. We've done that. We've seen, for example, that the renewal periods of certain key FISA orders may be longer than the initial periods. This makes sure the FBI can carry out missions, without providing value in the fight against terrorists.

Those of us who feel strongly about how law enforcement might chip away at traditional privacy rights will closely watch how law enforcement uses these tools.

The events of September 11 have changed us as a country forever. We have been attacked on our own soil. Thousands have died, thousands more have been injured. Very simply, we must do all that we can to stop terrorism by finding and disrupting terrorist activities here and abroad. The challenge we face is to do this without compromising the value that makes Americans unique and have allowed us to become great: respect for personal autonomy and the rights of the individual; and tolerance of all regardless of race or religion.

While I will vote for this bill, I also promise to engage in vigilant oversight of these new powers, and I urge those in the law enforcement and intelligence communities to use these powers wisely and with great deliberation.

Mr. EDWARDS. Mr. President, I rise in support of S. 1510, the Uniting and Strengthening America Act.

In the aftermath of September 11, we face two difficult and delicate tasks: to strengthen our security in order to prevent future terrorist attacks, and at the same time, to safeguard the individual liberties that make America a beacon of freedom to all the world.

I believe that when the President signs this anti-terrorism legislation into law, we will have achieved those two goals as best we now can.

The act is a far-reaching bill. I will mention just a few key aspects of that bill.

First, the legislation brings our surveillance laws into the 21st century. Here are two of many examples. Under current law, the FBI needs a basic search warrant to access answering machine messages, but the FISA needs a different kind of warrant to get to voice mail. This law says the FBI can use a traditional warrant for both. Another example: Under current law, a Federal court can authorize many electronic surveillance warrants only within the court's limited jurisdiction. If the target of the investigation is in the judge's jurisdiction, but the subject of the warrant is an Internet service provider located elsewhere, the warrant is no good as to that ISP. This bill allows the court overseeing an investigation to issue valid warrants nationwide.

Second, the act gives law enforcement officers and the foreign intelligence community the ability to share intelligence information with each other in defined contexts. For example, if they are not under special conditions, the FBI may share wiretap and grand jury information related to foreign and counter-intelligence. I appreciate concerns that this information-sharing authority could be abused. Like Chairman LEAHY, I would have preferred to see greater judicial oversight of these data exchanges. But I also believe we simply cannot prevail in the battle against terrorism if the right hand of our government has no idea what the left hand is doing.

Third, the act enhances intelligence authorities under the Foreign Intelligence Surveillance Act (FISA). When I met with FBI agents in North Carolina shortly after September 11, they told me their number one priority was to streamline the FISA process. We've done that. We've seen, for example, that the renewal periods of certain key FISA orders may be longer than the initial periods. This makes sure the FBI can carry out missions, not duplicative court applications.

A more controversial change concerns the purpose of FISA surveillance. Under current law, a FISA wiretap order may only enter if the primary purpose of the surveillance is foreign intelligence gathering. The administration initially proposed changing the "primary purpose" requirement to a "purpose" of "a purpose" and "foreign intelligence purpose." At a recent Intelligence Committee hearing, I was one of several Senators to raise constitutional questions about the Administration's initial proposal. The last thing we want is to permit FISA investigations lost, and convictions overturned, because the surveillance is not constitutional. S. 1510 says that FISA surveillance requires not just "a purpose," but "a significant purpose," of foreign intelligence gathering. That new language is a substantial improvement that I support. In applying this "significant purpose" requirement, the FISA court will still need to be careful to enter FISA orders only when the requirements of the Constitution as well as statute are met. The Department of Justice has stated in its letter regarding the proposed FISA change, the FISA court has "an obligation," whatever the statutory standard, "to reject FISA applications that do not quality as "significant purpose." I anticipate continued close congressional oversight and inquiry in this area.

A forth step taken by this legislation is to triple the number of Border Patrol, INS inspectors, and Customs Serv- ices agents along our 4,000-mile northern border. Today there are just 300 border patrol agents to guard those 4,000 miles. Orange cones are too often our only defenses against illegal entries. This bill will change that.

Finally, the bill makes the criminal law tougher on terrorists. We make it a crime to possess a biological agent or toxin in an amount with no reasonable, peaceful purpose, a crime to harbor a terrorist, a crime to provide material support to terrorism. And we say that when you commit a crime of terrorism, you can be prosecuted for that crime in the first year of your imitations period. Statutes of limitations guarantee what lawyers call "repose." Terrorists deserve no repose.

As Chairman LEAHY and Senator HATCH have both said, this legislation is not perfect, and the House-Senate Conference may yet make improvements. For example, the Conference might clarify that, as to aliens detained as national security threats, the law will secure the due process protections and judicial review required by the Constitution. In the Supreme Court's recent decisions in Zadvydas v. Davis and INS v. St. Cyr. The Conference might also sensibly include a
The bill is not perfect, but it is a good bill, it is important for the Nation, and I am pleased to support it.

Mr. KYL. Mr. President, I rise in strong support of the antiterrorism bill, S. 1510. The bill would provide our nation’s law enforcement with important tools to more effectively investigate and prevent further attacks against the people of the United States.

At the outset, in response to concerns that some have raised, I want to make clear that we are not rushing to pass ill-conceived legislation.

During the past two Congresses, when I chaired the Judiciary Committee’s Subcommittee on Technology and Terrorism, the Subcommittee held 19 hearings on terrorism. I want to repeat that: 19. The witnesses who appeared before the Subcommittee included the then-Director of the FBI Louis Freeh and representatives of all three of the congressionally-mandated commissions on terrorism that have issued reports over the past two years.

Many of the provisions contained in the Attorney General’s proposed legislation, the recommendation of one or more of the major terrorism commissions and have already been examined by the committee of jurisdiction. In fact, some of these provisions have already been voted on and passed by the Senate.

Indeed, as I will discuss more fully in a minute, the language sent forward by the Attorney General to establish nationwide trap and trace authority was included in the Hatch-Feinstein-Kyl Amendment to the recently passed Commerce, Justice, State Appropriations bill. Much of the remaining language in that amendment was included in the Counterterrorism Act of 2000, which the Senate passed last fall, after a terrorist attack on the U.S.S. Cole killed 17 American sailors and injured another 39. That bill was based on recommendations of the bipartisan, congressionally-mandated National Commission on Terrorism, known as the Brennan Commission, which was established in 1998 in response to the embassy bombings in Tanzania and Kenya.

One particularly important provision, which was included in the both the CJS bill and the current bill, updates the law to keep pace with technology. The provision on pen register and trap and trace devices 1. Would allow judges to enter pen/trap orders with nationwide scope and 2. Would codify current caselaw that holds that pen/trap orders apply to modern communication technologies such as e-mail and the Internet, in addition to traditional phone lines.

Nationwide jurisdiction for a court order will help law enforcement to quickly identify other members of a criminal organization such as a terrorist cell. Indeed, last year Director Freeh testified before the Terrorism Subcommittee that one of the problems law enforcement faced was the jurisdictional limitation of pen registers and trap-and-trace orders issued by federal courts.” [Source: Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, 106th Cong, 2nd Sess. (March 28, 2000), at 31.]

He continued: “Today’s electronic crimes, which occur at the speed of light, cannot be effectively investigated with procedural devices forged in the last millennium during the infancy of the information technology age.” [Source: Id. at 32.]

Currently, to track a communication that is purposely routed through Inter- net Service Providers in different states, law enforcement must obtain multiple court orders. This is because, under current law, a Federal court can order only those communications carriers within its district to provide tracing information to law enforcement.

According to Director Freeh’s testimony before the Terrorism Subcommittee, “As a result of the fact that investigators typically have to apply for the same order to trace a single communication, there is a needless waste of time and resources, and a number of important investigations are either hampered or delayed entirely in those instances where law enforcement gets to a communications carrier after that carrier has already discarded the necessary information.” [Source: Id. at 31.]

Section 216 of the Senate bill solves this problem.

I would also like to address another important provision.

Section 802 is intended more clearly to criminalize the possession of biological and toxin agents by those who should not possess them. This section amends the implementing legislation for the 1972 “Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological, Biological, and Toxin Weapons and on Their Destruction”, BW C. Article I of the convention applies to the development, production, stockpiling, acquisition, or retention of Microbial or other biological agents, or toxins, whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes. It is not the intent of the BWC, nor is it the intent of Section 802, to prevent the legitimate application of biological agents or toxins for prophylactic, protective, bona fide research, or other peaceful purposes. The section does not include, inter alia, medical and national health activities, and such national security activities as may include the confiscation, securing, and/or destruction of possible illegal biological substances.

Finally, let me address briefly the concern voiced by some that we are in danger of “trampling civil liberties.” I return to that argument, that we have had thorough, deliberative hearings, and that many of the proposals have already been passed by the Senate. Nothing in the current bill impinges on civil liberties. The bill would give Federal agents fighting terrorism the tools they would need to fight those fighting illicit drugs, or even postal fraud. Many of the tools in the bill are modernizations of the criminal laws, necessitated by the advent of the Internet.

While some of these tools are extremely helpful in terrorism investigations, it makes no sense to refuse to apply these common sense changes to other crimes that are committed, like kidnapping, drug dealing, and child pornography. It is absurd to limit these tools to only terrorism offenses because often, at the outset of an investigation of a particular person or crime, law enforcement does not know what you are dealing with. A credit card fraud case or a wiretapping documents case may turn out to be connected to funding or facilitating the operations of a terrorist group. We should give law enforcement the tools it needs to have the best chance of discovering and disrupting these activities.

We have a responsibility to the people of this nation to ensure that those who are charged with protecting us from future terrorist attacks are empowered to do so. This is not a zero sum game. We can both ensure our security and protect our liberties.

We cannot afford to lose this race against terror, and we cannot afford to give the enemy in this war a full lap head start. I support this bill. I commend President Bush and General Ashcroft for submitting a sound proposal to the Senate, and for their tremendous efforts during the past month.

Mr. President, in addition to the all of the other provisions in this antiterrorism legislation that will provide our law enforcement communities with the tools to weed out and stop terrorism, I want to express my support for the immigration provisions upon which the administration, Senators HATCH, KENNEDY, LEAHY and I have reached agreement, and which are included in this bill.

Even with the passage of these provisions, however, the United States will continue to face overwhelming infrastructure and personnel needs at our consular offices abroad, along both the southern and northern border, and in our immigration offices throughout the United States. In conjunction with increasing personnel and infrastructure, the administration must also improve the ability to present altered international documents, and improve the dissemination of information about suspected
terrorists to all appropriate agencies. Senator FEINSTEIN and I, in a hearing of the Terrorism Subcommittee of the Judiciary Committee this Friday, will continue to assess these needs by hearing from Justice and State Department officials.

So, our actions on immigration reform as it is relates to terrorism must go beyond the scope of this anti-terrorism package. With that said, this bill will certainly provide a better legal framework for keeping foreign terrorists out of the United States, and detaining them should they enter.

First, this antiterrorism bill clarifies that the Federal Bureau of Investigation is authorized to share data from its "most wanted list," and any other information contained in its national crime-information system, with the Immigration and Naturalization Service and the State Department. This will help the INS and State Department identify suspected terrorists before they come to the United States, and should they gain entry, will help track them down on our soil. It also allows the State Department, during a U.S. criminal investigation, to give foreign governments information on a case-by-case basis about the issuance or refusal to issue a U.S. visa.

The bill will also clarify U.S. law prohibiting the entry of, and requiring the removal of, individual alien terrorists. It will require the State Department of this body a great deal to know that, under current law, a terrorist alien is not considered either inadmissible to, or deportable from, the United States even if he or she has "endorsed or espoused terrorist activity that undermines the efforts of the United States to fight terrorism," or has provided "material support to a terrorist organization." Nor is an individual deportable for being a "representative of a terrorist organization." The anti-terrorism provisions of this bill will also make it clear that U.S. officials considering whether to allow someone to come to the country, that a person meeting any one of these criteria is not welcome here.

In addition, the anti-terrorism package that is being drafted today further defines what is considered by the United States to be a terrorist organization. Under current law, a terrorist organization must be designated by the Secretary of State under Section 219 of the Helms-Burton Act. This process can take several months, and has been criticized by some experts as potentially politically corruptible. Under this Senate anti-terrorism package, Section 219 remains in effect. A separate designation process is added, whereby an organization can be designated by the Secretary of State or the Attorney General, in consultation with each other, with seven days' notice to the leadership of the House and Senate, and the congressional committees of jurisdiction. Additionally, an organization, whether or not it is formally designated by the Secretary of State or the Attorney General, can be considered to be terrorist if it is made up of two or more individuals who commit or plan to commit terrorist activities.

The Senate's antiterrorism package also has provisions regarding temporary detention for the temporary detention of aliens who the Attorney General certifies that he has "reasonable grounds to believe is inadmissible or deportable under the terrorism grounds." This compromise represents the understanding that the Attorney General of the United States needs the flexibility to detain suspected terrorists. Under the compromise that Members have reached, the Attorney General must charge an alien with a deportable violation or he must release the alien. The underlying certification, and all collateral matters, can be reviewed by the U.S. District Court of the District of Columbia, and the Attorney General is required to report to Congress every six months on the use of this detention provision.

Finally, the Senate package, as a result of amendments added by Senator BYRD, will determine whether "consular shopping"—i.e., someone has a visa application pending from his or her home country, but goes to another country for adjudication—is a problem. If so, the Secretary of State must recommend ways to remedy it. Another provision authorizes $36.8 million for quick implementation of the INS foreign student tracking system, a program that I have repeatedly urged be implemented. As former chairman and now ranking Republican of the Judiciary Committee's Terrorism Subcommittee, I have long suggested, and strongly supported, many of the anti-terrorism and immigration initiatives now being advocated by Republicans and Democrats alike. In my sadness about the overwhelming and tragic events that took the lives of precious lives, I am resolved to push forward on all fronts to fight against terrorism. That means delivering justice to those who are responsible for the lives lost on September 11, and reorganizing the institutions of government so that the law-abiding can continue to live their lives in freedom.

Mrs. FEINSTEIN. Mr. President, I rise in strong support of the consensus terrorism bill now on the floor of the U.S. Senate.

The people of the United States awoke on September 12 to a whole new world, one in which we can no longer feel safe within our borders. We awoke to a world in which our very way of life is under attack, and we have since resolved to fight back with every tool at our disposal.

This is an unprecedented state of affairs, and it demands unprecedented action. We must seek out and defeat individuals and groups who would build upon the September 11 attacks with more of their own. We simply must give law enforcement officials the tools they need to track, to hunt down, and to capture terrorists, both in this country, and around the world as well. And that is what this bill would do.

Let me just describe some of the key provisions of this legislation, and how those provisions will make an impact, even in the current investigation into the September 11 attacks.

First, this bill makes it easier to collect foreign intelligence information under the Foreign Intelligence Surveillance Act, FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.

But in today's world things are not so simple. In many cases surveillance will have two key goals—the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary purpose" of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.

Rather than forcing law enforcement to decide which purpose is primary—law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.

The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.

This language is a negotiated compromise between those who wished the law to stay the same, and those who wished to virtually eliminate the foreign intelligence statutory language. The administration originally proposed changing "primary purpose" to "a purpose," but when I questioned Attorney General Ashcroft at our Judiciary Committee hearing, he agreed that "significant purpose" would represent a good compromise.

Second, this legislation will provide multi-point authority, or so-called "roving wiretap authority" in foreign intelligence investigations. This provision is designed to allow law enforcement to evade law enforcement by simply switching cell phones or moving locations.

Under current law, law enforcement must get a wiretap order for each individual's phone line. Criminals and terrorists know this, so they often manage to defeat surveillance by simply moving locations or exchanging cell phones.

This legislation will now allow the surveillance to follow the person, wherever or however that person is communicating. So, no longer will duplicative
wiretap orders be necessary simply to listen to the same, single target of an investigation. This is a powerful change to the law that does not put innocent conversations in danger, but stops the evasion of surveillance now possible under the law.

Third, this legislation allows nationwide service of so-called “pen register” and “trap and trace” orders. Those orders allow law enforcement to track incoming and outgoing phone calls, and now wiretaps are easier to get, so that authorities can make connections between various criminals or terrorists.

The problem with current law is that it has not kept up with technology. Modern technologies travel through many jurisdictions before reaching their final destinations, and current law requires court orders from every jurisdiction through which the communication travels. Under this legislation, only one court order will be necessary, eliminating the time-consuming and burdensome requirements now placed on law enforcement simply because technology has changed the way communication travels from one place to another. Law enforcement resources should be spent in the field, not filing unnecessarily burdensome motions in courtroom after courtroom.

I should also mention one important point about this provision. The standard necessary to get a court-ordered pen register or trap and trace is lower than the standard necessary to get a wiretap, so it was very important to make sure that this legislation makes it clear that these orders do not allow law enforcement to eavesdrop on or read the content of communication. Only the origin and destination of the messages will be intercepted.

This legislation also authorizes the seizure of voice-mail messages pursuant to a probable cause warrant, which is an easier standard for law enforcement to meet than the standard required for a wiretap. Current law treats a voice-mail like an ongoing oral conversation, and requires law enforcement to obtain a wiretap order to seize and listen to those saved messages. E-mails, however, receive no similar protection. In my opinion, if law enforcement can access e-mail communications with probable cause, the same should be the case with voice-mails. And so it will be once this legislation passes.

This legislation will also now allow for limited sharing of grand jury and other criminal investigation information with the intelligence community, to assist in the prevention of terrorist acts and the apprehension of the terrorists themselves.

Under current law, law enforcement officials involved in a grand jury investigation cannot share information gathered in the grand jury with the intelligence community, even if that information would prevent a future terrorist act.

Under this legislation, grand jury and other criminal investigative information can be shared if one, the information can be foreign intelligence and counterintelligence information, as defined by statute; two, the information is given to an official with a need to know in the performance of his or her official duties; and three, the limitations on public or other unauthorized disclosure would remain in force.

This balance makes sense. I believe strongly that grand jury information should not be leaked to the public or disclosed haphazardly to anyone. But at the same time, it makes perfect sense to allow our own law enforcement officials to talk to each other about ongoing investigations, and to coordinate their efforts to capture terrorists wherever they may be.

This legislation also contains a heavily negotiated provision regarding the detention of aliens suspected of links to terrorism without charging them. Agreement was reached to limit to 7 days the length of time an alien may be held before being charged with criminal or immigration violations, two, allow the Attorney General to delegate the certification power only to the INS Commissioner, and three, specify that the merits of the certification is subject to judicial review.

This legislation also contains several key provisions from a bill I introduced last month with the chairman of the Intelligence Committee, Senator Graham. For instance, the bill clarifies the role of the CIA director as the coordinator of strategies and priorities for how the government uses its limited surveillance resources; requires that law enforcement officers who discover foreign intelligence information in the course of a criminal investigation share that information with the intelligence community; includes “international terrorist activities” in the definition of “foreign intelligence” to clarify the authorities of the CIA; includes a provision that the CIA should make efforts to recruit informants in the fight against terrorism, even if some of those informants may, as is likely the case, not be ideal citizens; requires a report from the CIA on the feasibility of establishing a virtual translation center for use by the intelligence community, so that translators around the country can assist in investigations taking place far, far away. For instance, this center could be located in Los Angeles to assist law enforcement in New York without even leaving California; and finally, agreement was reached to require the Attorney General, in consultation with the CIA Director, to provide training to federal, state and local government officials to identify foreign intelligence information obtained in the course of their duties.

In addition, this bill also: Triples the number of Border Patrol, Customs Service, and INS inspectors at the northern border; authorizes $50 million to improve INS and Customs technology for monitoring the northern border and to add equipment on the border; lifts the statute of limitations on terrorist acts as defined by law where those crimes resulted in, or created a risk of, death or serious bodily injury. These crimes include bio-terrorism, attacks against airports and airplanes, arson or bombings of U.S. facilities, and other terrorist acts; adds this same list of terrorist crimes certain as predicates for RICO and money laundering; creates two new bio-terrorism crimes, the first prohibits certain described acts with non-resident aliens from countries that support terrorism, from possessing a listed biological agent or toxin; and the second prohibits any person from possessing a biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by a peaceful purpose.

The Attorney General and the President of the United States have asked this Congress to pass legislation that will assist in the war against terrorism, and I am one who believes very strongly that we should do so, and we should do so quickly.

This bill is a product of intense negotiation, and I believe that a good balance has been struck here. Compromises have been reached on the most controversial provisions, roving wiretap authority; trap and trace of computer routing information; sharing of grand jury information; and mandatory detention of aliens suspected of terrorism.

Although I no longer believe it to be necessary now that these compromises have been reached, I would support a five-year sunset on the provisions I just mentioned as a valuable check on the potential abuse of the new powers granted in the bill.

But a two-year sunset, such as the one contained in the House bill, is simply too short to allow law enforcement to accomplish what it needs to do to rout terrorists from this country.

The legislation before us contains provisions that could actually help in the current investigation into Osama bin Laden and his network in the United States and abroad.

I urge this Senate to pass this legislation and get it to the President for his signature. We are in a sustained war against terror, and we have waited long enough. I urge this Senate to pass this legislation and get it to the President for his signature.

FISA AND PEN REGISTER/TRAP AND TRACE

Ms. CANTWELL. Mr. President, I would like to raise several concerns regarding the provisions of this legislation, the USA Act of 2001, that expand wiretapping authority under the Foreign Intelligence Surveillance Act of 1978, and amend Federal pen register and trap and trace authorities.

Both of these changes purport to improve communication between law enforcement and intelligence operatives. There is a difference, however, between facilitating the sharing of information between the law enforcement and intelligence communities, and blurring the
line between the missions of the two communities. Where information is sought for the purpose of law enforcement, we must ensure that fourth amendment protections apply. Much of the fear about the legislation is based on legitimate concerns that law enforcement, gathered ostensibly for intelligence and defense purposes could be used for law enforcement purposes. The intelligence community does not prosecute and lock up its targets; it uses information, instead, to assist national security. The differences in these missions must be acknowledged, and we must be vigilant to maintain the distinction.

We can all agree that the events on September 11 have focused America on the need for our priority to shift from law enforcement to protection of citizens. But the law enforcement community has a different mission, to catch and prosecute criminals in our courts of law. Because law enforcement acts upon U.S. citizens, it must do so within the bounds of the Constitution. The differences in these missions must be acknowledged, and we must be vigilant to maintain the distinction.

I appreciate Chairman Leahy's tireless efforts to facilitate our intelligence gathering authorities, while preserving our constitutional rights. The negotiations have been intense, but these are difficult and divisive issues. Given the time frame, Chairman Leahy's charge has not been an easy one, but I appreciate the substantial progress he has made.

I remain concerned that some of the legislative changes fail to balance the increased powers to law enforcement against the need to protect the civil liberties of Americans. With these changes to FISA, it will be much more likely that the FBI will be able to obtain secret FISA wiretaps on American citizens. That information may not only be used for intelligence purposes, but also in a criminal prosecution, without complying with the normal requirements of a title III wiretap and the safeguards it provides to adhere to the fourth amendment. Some have warned that this language leaves room for fishing expeditions rather than providing to the Committee at the request of our Members does not even attempt to justify the original proposal, but instead presents argument for why a change to a "significant" purpose would be constitutional.

I remain disappointed with the administration's insistence on forcing any change on this important statutory requirement. FISA was enacted for the express purpose of clarifying that different legal standards apply to those gathering foreign intelligence than to those seeking criminal evidence. This new provision will blur that distinction, and it is indeed very problematic in my mind.

Federal courts have upheld FISA on the basis that what is reasonable under the fourth amendment may vary when national security is at risk. Thus, a FISA wiretap does not have to be based on probable cause to believe a crime has been or is about to be committed, and no notice is given unless the person is present in the home, while judges review warrants on the merits when targets are U.S. persons, the primary purpose for the wiretap must be the protection of our national security. Upon satisfaction of that critical condition, the statute authorized the use of evidence obtained under a FISA wiretap for criminal prosecution.

Ms. Cantwell. Mr. President, although much effort has gone into narrowing this provision to fit within the bounds of the Constitution, it would seem to me that this legislation may not stand up to this test, and thus may fail judicial scrutiny. Regardless, we cannot await court review. I believe Congress must keep watch over the use of technologies such as the FBI's "Carnivore" to access information that is protected by the fourth amendment. The failure to properly define the term "address" in the e-mail context to exclude information protected by the fourth amendment will haunt us for a long time. And I regret this. Although it certainly can be said that new technologies are emerging and the definition may need be flexible, the term "address" presently is undefined and wide-ranging in the current Federal criminal statutes. Because of this ambiguity, we may see law enforcement authorities take inconsistent approaches to filtering information pursuant to this new law. There is risk that some will obtain information, such as "subject line" information or URL codes, that may otherwise be protected by the fourth amendment. There is certainly to be judicial scrutiny of this provision.

Mr. LEAHY. I agree with you completely, and you can rest assured that the Judiciary Committee under my chairmanship will conduct meaningful oversight, as we already have begun to do over the summer.

Although FISA requires oversight reporting to the Intelligence Committees, the law makes it clear that other committees may also have oversight jurisdiction. Section 108 of FISA, 50 U.S.C. 1808, states, "Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of Congress to obtain such information as they may need to carry out their respective functions and duties." Section 306 of FISA, 50 U.S.C. 1826, provides for semiannual reports from the Attorney General to the Intelligence and Judiciary Committees on the number of applications for physical search orders made, granted, modified, or denied, and the number of physical searches which involved the property of United States persons. The Judiciary Committee's responsibility will be greater under the amendment to FISA, because of the greater authority to use FISA for law enforcement purposes.
nation with such a report, so I would be content with closed-session hearings on the findings of such reports. But only with such oversight can we reasonably assure our constituents that the use of these new authorities is not impinging on our legitimate concern to preserve our fundamental rights.

Mr. LEAHY. I agree with Senator CANTWELL and I appreciate her efforts to suggest restraint at the Department of Justice to avoid misusing the new authorities we are contemplating using to address terrorism. I share her view that the GAO should undertake this important assignment and will work with her and other Senators to see it accomplished. We all need to make certain that these new authorities are not abused.

Mr. CANTWELL. I thank the chairman for his diligence in working to preserve our fundamental rights.

Mr. ENZI. Mr. President, I am proud to be a co-sponsor of S. 1510, the “Uniting and Strengthening America Act” or “USA Act.” This bill reflects a bipartisan effort to aid law enforcement, immigration, and the intelligence community in investigating, detaining, and apprehending suspected terrorists. This legislation follows lengthy committee inquiry and revision of a proposal Attorney General Ashcroft proposed a few weeks ago and which sparked national debate over whether civil rights would be violated.

During the past few weeks, Senate leaders on both sides of the aisle, working tirelessly with Attorney General Ashcroft in order to create a bill that strengthens our existing laws with respect to apprehending terrorists, but still protects the civil rights of our citizens. This is an important mission for Congress. Everyone in America understands the need for enforcement, immigration and the intelligence community to have the tools necessary to find terrorists, cut-off their financial support, and bring them to justice.

While I am committed to routing out terrorists here and abroad, I am equally committed to making sure the rights of innocent U.S. citizens are not violated. This includes the privacy and property rights our constitution affords and that make this country so great. I believe this bipartisan bill does both. This legislation strikes a balance between protecting our civil rights and assisting Attorney General Ashcroft and other federal, state and local government agencies in their anti-terrorism efforts. State and local law enforcement have a critical role to play in preventing and investigating terrorism, and this bill provides them benefits appropriate to such duty. The bill streamlines and expedites the Public Safety Officers’ Benefits application process, provides a supplemental payment for family survivors of firefighters, police officers and other emergency personnel who are killed or suffer a disabling injury in connection with a future terrorist attack. And it raises the total amount of the Public Safety Officers’ Benefit Program payments from approximately $150,000 to $250,000.

This bill will also make an immediate difference in the lives of victims of terrorism and their families. It reauthorizes, expands, and by adding in our bill, pre-dating it, so improves the way in which its crime fund is managed and preserved. It replenishes the emergency reserve of the Crime Victims Fund with up to $50 million and improves the mechanism to replenish the fund in future years. The USA Act also increases security on our Northern Border, including the border between Canada and my State of Minnesota. It triples the number of Border Patrol, Customs Service and INS inspectors. The Northern Border and Mathematical $100 million to improve old equipment and provide new technological equipment to INS and the Customs Service at that border.

On the criminal justice side, the bill clarifies existing “cybercrime” law to cover computers outside the United States that affect communications in this country and changes sentencing guidelines in some of these cases. It provides regulatory targets to go after those involved in money-laundering schemes that are linked to terrorism, and it adds certain terrorism-related crimes as predicates for RICO and money-laundering. It creates a new statute targeting state and local terrorism on mass transportation systems, and it strengthens our Federal laws relating to the threat of biological weapons. The bill will enhance the Government’s ability to prosecute suspected terrorists in possession of biological agents of a type or quantity that is not reasonably justified by a peaceful purpose.

The bill also broadens the authority of the President to impose sanctions on the Taliban regime. Regarding criminal penalties for those convicted of terrorism, the bill removes the notion of what constitutes “terrorism” and ensures that penalties more closely reflect the offenses committed by terrorists. Again, I’d like to thank my colleagues from Vermont and others who have worked with me on these provisions. The administration’s initial proposal was too broad in this area, and the current bill provides a fair alternative.

I strongly support these needed provisions. Still, I do have concerns about the possible effect on civil liberties of the bill’s measures to enhance electronic surveillance and information sharing of criminal justice information, while at the same time reducing judicial review of those actions. I also believe that the bill’s provisions to expand the Government’s ability to conduct secret searches, as well as searches under the Foreign Intelligence Surveillance Act, will not be abused.

I believe we will need to monitor the use of new authorities provided to law enforcement agents to conduct surveillance of internet communications. The same is true of the bill’s changes to laws allowing the sharing of confidential criminal justice information with various Federal and state agencies. I applaud the requirement of judicial review before disclosure, which is contained in the House version of this bill. Likewise, I believe the House of Representa-tives’ decision not to include this bill’s expansion of the Government’s ability to conduct secret, or so-called “Sneak-n-Peek,” searches, was correct. I hope the safeguards against abuse we have added in our bill—such as the prohibition against the Government seizing any tangible property or stored electronic data or communications without a showing of reasonable necessity, as well as the requirement that notice be given within a reasonable time of the
The bill broadens the Foreign Intelligence Surveillance Act, FISA, by extending FISA surveillance authority to criminal investigations, even when the primary purpose is not intelligence gathering. The bill limits this ability by authorizing surveillance only if a significant purpose of it is to gather intelligence information. I hope this new FISA authority will be used for the purpose of investigating and preventing terrorist acts and not for other domestic purposes.

Mr. President, we have done our best in this bill to maximize our security while minimizing the impact some of these changes may have on our civil liberties. Nearly all of us have probably said since September 11 that if that day's terror is allowed to undermine our democratic principles and practices, then the terrorists will have won a victory. I hope we can pass this bill today. And we should also commit ourselves to monitoring its impact on civil liberties in the coming months and years.

I believe a sunset provision that ensures that review is essential. The bill before us today is good, but there are provisions that are too broad. There are parts that should be more narrowly focused on combating terrorism. I hope these are the concerns that will be addressed in conference. Mr. President, our challenge is to balance our security with our liberties. While it is not perfect, I believe we are doing that in this bill.

To more effectively fight terrorism and those who perpetrate it, we need to improve law enforcement's intelligence gathering capability and enhance their ability to investigate and prosecute suspected terrorists. This measure does both. But let's also be realistic about the act. It will not solve all of law enforcement's problems in combating terrorism nor will it severely compromise our civil liberties. The truth lies somewhere in between.

The strongest proponents of the legislation argue that the bill primarily consists of long overdue updates of current laws, updates necessary because technology have advanced criminals and terrorists to stay a step, or two, ahead of law enforcement. Updates are necessary because the inability of Federal authorities to share information on suspected terrorists hampers criminal investigations. Updates are necessary because the penalties and limitations periods governing many terrorist crimes have been woefully inadequate. All of this is true. And for these reasons, I support the bill.

But my purpose is not to indulge in thinking that this measure will solve our problems. Indeed, I asked the Attorney General whether the new powers granted in this bill could have prevented the events of September 11. He answered me honestly, saying that he could not make that guarantee. Yet, he added that these new tools would make it less likely that terrorism could strike in the same way again.

Tougher penalties are an important part of our strategy to combat terrorism. That plan must also include more and better agents dedicated to gathering intelligence, an aggressive approach to preventing attacks, and patience from all Americans. Patience is not one of our natural virtues. We need to understand that we might have to temper our freedoms slightly in an effort to guarantee them.

Critics of this legislation caution us to be wary of compromising our liberties in an effort to make our Nation safer. They comment that sacrificing freedom gives the terrorists a victory. Those warnings do have merit.

Some of this bill's provisions do risk our civil liberties and ask Americans to commit criminal activity. This bill grants our prosecutors a great deal of discretion in enforcing the law and asks Americans to have faith that this power will not be abused. Most of us would rather not have our civil liberties depend on someone else's discretion.

That's why I believe many of this bill's provisions should lapse in two years and then be reconsidered by Congress. The House version of this bill recognizes the need for tough law enforcement with the concern for our civil liberties by sunsetting some of the most objectionable portions of the bill in two years. That is a good idea. Two years from now, we can take stock of where we are, how this bill has affected us, and whether the trust we show in law enforcement is warranted. I hope that the final version of this bill will adopt such a sensible approach.

I have never doubted that our country's leadership will be focused on the terror threat in the world. They are dedicated, creative, committed, and decent. From local beat officers to the Director of the FBI, every one of them has a vital role to play in combating terrorism. We believe this bill will help them prevent terrorism when possible. It will help them catch wrongdoers. It will cut wrongdoers off from their support networks. It will guarantee stiff punishment for their criminal acts. It will deter others from following in the terrorists' footsteps. It is our responsibility to give law enforcement the tools they need in an increasingly complex world. It is their responsibility to use them wisely.

Mr. SADLER. Mr. President, I rise today in support of the antiterrorism legislation we have before us.

First, let me say I am pleased to have also worked in conjunction with Senator BOND and Senator CONRAD in supporting their legislation entitled 'The USA Intelligence Act.' This bill addresses many of the concerns I have, such as the importance of information sharing among Government law enforcement and intelligence agencies with the State Department and tightening tracking controls on those entering the United States on student visas, including those attending flight schools. These are critical issues, and I commend both Senators for their efforts.

Today, our men and women in uniform are on the frontlines in the war against terrorism. We salute their willingness to put themselves in harm's way in defense of freedom, and we pray for their safety and for the safety of everyone at home, we are working to secure our nation, and that is why I am pleased that we will pass this legislation in the Senate that will take strong measures to help prevent further terrorist attacks on American soil.

With this legislation, we will take reasonable, constitutional steps to enhance electronic and other forms of surveillance, without trampling on the rights of Americans. We will also institute critical measures to increase information sharing by mandating access to the FBI's National Crime Information Center, or NCIC, by the State Department and INS.

In our war against terrorism, America stands as one behind our President. It is equally critical that, in the all-out effort to protect our homeland, Federal agencies be united in securing American soil.

In that light, President Bush made exactly the right decision when he created the Office of Homeland Security, a national imperative in the wake of the horrific tragedies of September 11, and I commend him for appointing my former colleague, Pennsylvania Governor Tom Ridge, as its Director.

With a seat at the Cabinet table, Governor Ridge will literally be at the President's side, giving him the standing that will be required to remove jurisdictional hurdles among the 40-plus agencies he will be responsible for coordinating. Now, we will assist in that coordination by allowing INS and the State Department access to the information they need to make informed decisions about who we will grant entrance into this country.

I saw firsthand the consequences of serious inadequacies in coordination and communication during my 12 years as ranking member of the House Foreign Affairs International Operations Subcommittee and Chair of the subcommittee's Senate counterpart. In fact, I recently wrote an op-ed piece concerning my findings during that time and I would like to submit the entire text of that piece for the RECORD.

In conducting oversight of Embassy security as well as visa and consular operations, I became extensively involved with the issue of terrorism, co-drafting antiterrorism legislation with former Representative Dan Mica in the wake of 1983 and 1984 terrorist attacks against the U.S. Embassy and Marine barracks in Lebanon—travelling to Belgrade, Warsaw, and East Berlin to press government officials into helping
stem the flow of money to the terrorist Abu Nidal and his organization—and investigating entry into the United States by radical Egyptian cleric Sheikh Omar Abdel Rahman, mastermind of the 1993 World Trade Center bombing.

As far back as our hearings on the 1985 Inman Report, commissioned by then-Secretary of State George Shultz in response to the attacks in Lebanon, it was abundantly clear that improved coordination and consolidation of information from agencies such as the FBI, CIA, DEA, Customs, INS and the State Department would be an essential step toward removing a vulnerability in our national security. That point was tragically underscored by our discovery that, astoundingly, in the period since 1987 when Sheikh Rahman was placed on the State Department lookout list, the Sheikh entered and exited the United States five times totally unimpeded.

But worse, however. Even after the State Department formally issued a certification of visa revocation, he was granted permanent residence status by the INS. When he was finally caught on July 31, 1991, reentering the United States, he was immediately released back into U.S. society to allow him to pursue a multi-year appeal process.

As unbelievable as that may sound, just as unfathomable is the fact that, even after the 1993 attack on the World Trade Center, membership in a terrorist organization in and of itself—with the exception of the PLO—was not sufficient grounds for visa denial. Rather, the Immigration Act of 1990 required the Government to prove that an individual either was personally involved in a terrorist act, or planning one.

This absurd threshold made it almost impossible to block individuals, such as Sheikh Rahman, from entering the country, while legislation I introduced a bill that would have required the State Department to jointly create an electronic database of unauthorized entries into the country. That provision was enacted in 1994 to respond to the attacks in Lebanon, but was later made optional and ad hoc.

Recognizing the need to mate these errors we uncovered requiring modernization in the State Department’s antiquated microfiche “lookout” system to keep dangerous aliens from entering the United States, I introduced a provision that would require the INS to use as well. When a foreign national receives a visa, a fingerprint is taken, and while my requirement for non-immigrant visas eventually used by all 19 suspected hijackers.

Also of note, we discovered later in trying to understand some of what happened during the 1993 attack that limited law was sunsetting in 1997 due to a provision added by the House-Senate conference on the Foreign Relations Authorization Act for FY 1994–1995—a conference of which I was not a member. Subsequently, that law was extended to 1998 in the Commerce-Justice-State Appropriations bill for fiscal year 1998, and then was allowed to expire. This happened despite my legislation enacted in 1996 eliminating the requirement that visas be processed by INS before being used by the State Department to deny visas. Tellingly, after it lost access to the NCIC, the visa denial rate for past criminal activities plunged a remarkable 45 percent—stark evidence that we can’t afford to tie the hands of America’s overseas line of defense against terrorism.

Incredibly, while intelligence is frequently exchanged, no law requires agencies like the FBI and CIA to share information on dangerous aliens with the State Department. To address this, my 1993 bill also designated the State Department a “law enforcement agency” for purposes of accessing the NCIC as well as other FBI criminal records and criminal records, whether immigrant or non-immigrant.

Unfortunately, a revised provision also enacted in 1994 only provided the State Department with free access to these FBI resources for purposes of processing immigrant visas—dropping my requirement for non-immigrant visas. Thus, today, information sharing remains impossible for non-immigrants to pay for the upgrades.

The required manual searches, was difficult to use, and was subject to error. The language I crafted required the State Department to replace the old systems with one of two forms of state-of-the-art computerized systems. Visa applicants would be informed of the reason for a denial—a provision that law enforcement agencies legitimately believed could impede ongoing investigations, or reveal sources and methods. Thus, today, information sharing remains optional and ad hoc.

Currently, U.S. post check the lookout database called the “Consular Lookout and Support System—Enhanced,” or CLASS-E, prior to issuing any visa. CLASS-E contains approximately 10 million records of which originate with U.S. embassies and consulates abroad through the visa application process. The INS, DEA, Department of Justice, and other Federal agencies also contribute lookouts to the system, however, this is voluntary.

The system, however, this is voluntary. To further fortify our front-line defenses against terrorism—to turn back terrorists at their point of origin—information sharing should be mandatory, not voluntary. That is why I introduced a bill that would require the law enforcement and the intelligence community share information with the State Department and INS for the purpose of issuing visas and permitting entry into the United States. And while my bill would have gone farther than the legislation before us—including the DEA, CIA, Customs and the Department of Defense in the mandated information-sharing network—I again emphasize that this legislation does mandate access to the NCIC by INS and the State Department.

Clearly, the catastrophic events of September 11 have catapulted us into a different era, and everything is forever changed. We must prove to and from the earth to remove the impediments that keep us from maximizing our defense against terrorism. The bottom line is, if knowledge is power, we are only as strong as the weakest link in our information network—therefore, we must ensure that the only “terror war” will be the one to protect American turf.

That is why we need a singular, Cabinet-level authority that can help us understand, and why we need legislation to help them do it. Ironically, the most compelling reason for an Office of Homeland Security is also its greatest challenge—the need to focus on the “whys” of communication and cooperation so that all our resources are brought to bear in securing our Nation.

Winston Churchill, in a 1941 radio broadcast, sent a message to President Roosevelt saying, “Give me the tools and we will finish the job.” I have no doubt that, given the tools, the men and women of our Embassies throughout the world will get the job done and help us build a more secure American homeland.

Finally, once a visa is issued at the point of origin, we should be ensuring that it’s the same person who shows up at the point of entry. The fact is, we are verifying the identity of the 19 terrorists implicated in the September 11 attacks entered the United States on visas that were actually issued to someone else.

Currently, once a visa is issued by the State Department, it then falls to INS officials at a port-of-entry to determine whether to grant entry. The problem is, no automated system is utilized to ensure that the person holding the visa is actually the person who was issued the visa. In other words, the INS official has to rely solely on the identification documents the person seeking entry is carrying—making that officials job that much more difficult.

The should be the one to verify that the person receiving the visa is the same person at the border crossing station trying to enter the country.

Simply put, it requires the State Department and INS to jointly establish a fingerprint-based check system to be used by State and INS to verify that the person who received the visa is the same person at the border crossing station trying to enter the country.

S10596 CONGRESSIONAL RECORD—SENATE October 11, 2001
the United States. This is a common sense approach that would take us one step closer to minimizing the threat and maximizing our national security.

The fact of the matter is, fingerprint technology—one part of the larger category of biometric technologies that can be used for identification known as biometrics—is not new. In fact, the U.S. Government has already employed biometrics to verify identities at military and secret facilities, at ports-of-entry, and for airport security, among many other things.

The INS has already announced it was beginning to implement the new biometric Mexican border crossing cards as required by 1996 Illegal Immigration Reform and Immigrant Responsibility Act. These cards have the individual’s fingerprint encoded on them and are matched to the fingerprint of the person possessing the card at a U.S. port-of-entry.

This surely does not sound all that much different than what I proposed. I am pleased the bill before us at least starts us down the road toward implementing biometric technologies by requiring a review of the feasibility of instituting such technology. Hopefully, the improvement can be achieved as soon as possible.

Despite areas where I might have wished to strengthen this bill even further, this legislation is vital to our national security, and I will be proud to support it. The war on terrorism is a war on myriad fronts. Some of the battles will be great in scale, many will be notable by what is not seen and by what doesn’t happen—namely, that individuals who pose a serious threat to this Nation never see these shores and never set foot on our soil.

Many of our greatest victories will be measured by the attacks that never happen—in battles we win before they ever have a name—in conflicts we prevent. I will be proud to claim one of those victories as a part of American life. I hope we will pass and enact legislation that will help make that possible. I thank the Chair.

Mr. KENNEDY. Mr. President, a month ago today, America was attacked by vicious terrorists bent on doing all they can to undermine our Nation, our freedoms, and our way of life. But they have failed. Our country has never been more united behind the ideals that make us strong, or more committed to protecting our security.

In the wake of the terrorist attacks of September 11, the American people have sought international cooperation and received it. We have asked our men and women in uniform to protect and defend our Nation, and they are doing it superbly. We are equally committed to preserving our freedoms and our democracy.

The goal of this antiterrorism legislation is to achieve greater coordination between the law enforcement and intelligence communities, while protecting the civil liberties of American citizens. We must give the Secretary of State and the Attorney General the tools to stop terrorists from entering our country, while guaranteeing America’s proud tradition of welcoming immigrants from around the world.

The terrorist attacks of September 11 make it an urgent priority to act as soon as possible. The INS and the State Department, the FBI, the National Security Agency, and intelligence information they need to make quick and accurate decisions on whether to admit anyone to the United States. We must also take urgent steps to improve security at our borders with Canada and Mexico, to keep terrorists from entering the country illegally.

These improvements in the immigration laws can make a huge and immediate difference. Immigration security is an indispensable part of our national security.

As we protect our country, we must also protect the founding principles that have made our nation great. We must respond to the current crisis in ways that protect the basic rights and liberties of our citizens and others residing legally in the United States.

Currently, the INS has broad authority to act against any foreign national who supports terrorism. With respect to visitors, foreign students, and other non-immigrants already in this country, the Federal Government has a broad range of enforcement tools. The INS may detain certain non-citizens if they pose a threat to national security or are a flight risk, and they may do so on the basis of secret evidence. The INS may also deport any alien who has engaged in terrorist activity, or supported terrorist activity in any way. If the INS has the resources to use its existing authority fully and fairly, we will be far closer to ensuring our national security.

Nonetheless, loopholes may exist in our current laws, and we should close them. In recent weeks, many of us in Congress have worked closely with the administration to strengthen the law without creating serious civil liberties concerns. Although we have made progress, more remains to be done. I continue to be concerned that the Attorney General has the authority to detain even permanent residents without adequate cause, and with very few due process protections.

We must be cautious that new measures are not enacted in haste, undermining America’s constitutional protections.

Consistent with these basic principles, it is essential for Congress to strengthen the criminal code in response to the September 11 attacks. We must increase penalties for terrorists and those who support terrorist activity. We must punish those who possess biological weapons and commit acts of violence against mass transportation systems. We must also ensure that victims of hate crimes are provided with aid and that civil liberties protection. However, I am confident that working with the House of Representatives and the administration, we can enact a final bill that makes it easier for the Department of Justice to prosecute hate crimes—while still ensuring that the Federal Government is only involved when necessary and appropriate.

Congress and the President must send a strong and unequivocal message to the American people that hate-motivated violence in any form will not be tolerated in our nation.

There are provisions in the Uniting and Strengthening America Act that do not strike the correct balance between law enforcement authority and civil liberties protection. I am concerned, however, that by authorizing foreign-intelligence searches where foreign-intelligence gathering is only “a significant purpose”—not the sole or primary purpose—of the search, the bill may well make the Foreign Intelligence Surveillance Act unconstitutional under the fourth amendment.

We must also ensure that, in acting to expand the powers of law enforcement to obtain student educational records for the investigation and prosecution of terrorism, we adequately safeguard the interests of innocent students. We should not permit schools and colleges to transfer student records to law enforcement agencies indiscriminately. We have worked closely with the administration to develop language that strikes a balance between the legitimate interests of law enforcement and the privacy of students.

In the wake of the September 11 attacks, we have also seen a disturbing increase in hate-motivated violence directed at American Muslims. The Department of Justice is currently investigating over 90 such incidents, including several murders.

We need to do more to combat the acts of hate that cause many Arab and Muslim Americans to live in fear. Under current law, the Department of Justice cannot prosecute such cases as hate crimes unless it can prove that the victim was engaged in one of six “federally protected activities”—such as voting or attending a public university—when the crime occurred. This requirement is an unwise and unnecessary constraint on effective law enforcement and may hamper the Department’s ability to prosecute some of the cases that are now involving hate.

The bipartisan hate crimes bill passed by the Senate last year and approved again by the Judiciary Committee in July would remove the “federally protected activity” requirement from the law—making it easier for the Justice Department to prosecute hate crimes—while still ensuring that the Federal Government is only involved when necessary and appropriate.

Congress and the President must send a strong and unequivocal message to the American people that hate-motivated violence in any form will not be tolerated in our nation.

There are provisions in the Uniting and Strengthening America Act that do not strike the correct balance between law enforcement authority and civil liberties protection. However, I am confident that working with the House of Representatives and the administration, we can enact a final bill that meets these important concerns.

I hope we will pass and enact this important legislation, send a strong message to the American people that hate-motivated violence in any form will not be tolerated in our nation.

I thank the Chair for the opportunity to introduce the victim compensation component of the hate crimes legislation.
Mr. KERRY. Mr. President, I am very pleased to have the opportunity to speak for a few minutes about the Uniting and Strengthening America, USA, Act, before the Senate today. This legislation reflects the hard work of the Senate Banking Committee and the Senate Judiciary Committee, and I want to thank them for their commitment to ensuring that Congress address this legislation as quickly as possible and send the bill along to the American people.

Right now our Nation is strongly united. We are bound together, among other things, a desire to see justice brought to those who planned the terrorist attacks and those who aided and abetted the terrorists. And Americans are united by our desire to prevent future terrorist attacks. At this time, more so than at any time in the past 40 years, the American people are standing firmly behind the Federal Government and they trust government to do the right thing. The American people support the idea that we must provide the FBI and the Department of Justice with the tools necessary to punish the perpetrators of the terrorist attacks and to prevent future attacks.

But as much as the American people seek a just resolution to the acts of terror, they are adamantly about protecting their rights and liberties. We have heard it time and again since September 11: our Nation must be secure, but must not become so at the expense of our freedoms, our rights, and our liberties. We must not let the American people down.

I want to thank Senator LEAHY for his leadership on this legislation and his concern with important Constitutional principles, such as due process and unreasonable search and seizure. At Senator LEAHY’s urging, the administration’s anti-terrorism proposal was carefully and closely analyzed and Senator LEAHY did not yield to the political pressures that threatened to push this legislation through the Congress without its careful consideration. I believe that the bill before the Senate is vastly improved from the proposal that is before the Senate Banking Committee last week. Today’s financial volume of laundered money is estimated to be 2 to 5 percent of global Gross Domestic Product, between $600 billion and $1.5 trillion. The effects of money laundering extend far beyond the parameters of law enforcement, creating international anti-money laundering and the Pentagon with funding that was used to develop a worldwide terrorist network, known as al Qaeda, have been included in this legislation is to give the Treasury Secretary, in conjunction with other allies in the European Union and the Financial Action Task Force, the authority to license U.S. banks to foreign anti-money laundering laws or standards to financial institutions with lax money laundering laws. If the proceeds of money laundering are used to finance terrorist activities, they must be stopped. The United States has declared a war on terrorism. This new war is going to be unlike anything that we have ever face. The world is the fight against terror, we must insure that our own laws are worthy of the difficult task ahead.
It provides a clear warning to those who have assisted or unwittingly assisted those involved in the al Qaeda network or other terrorist organizations in laundering money. The United States will take whatever actions are necessary, including denying them bank accounts or other financial transactions, access to the United States economy, in order to stop terrorists and international criminal networks from continuing to launder money through the international financial system.

Passage of this legislation will make it much more difficult for new terrorist organizations to develop. During the 1980s, as Chairman of the Senate Permanent Subcommittee on Investigations, I began an investigation of the Bank of Credit and Commerce International (BCCI), and uncovered a complex money laundering scheme involving billions of dollars. Fortunately, BCCI was forced to close and we were able to bring many of those involved in to justice. However, as we have learned since the closing of BCCI, Osama bin Laden had a number of accounts at BCCI and we had dealt him a very serious economic blow. So as we consider this bill as a response to recent attacks, we lose sight sight of the potential this legislation will have to stop the development of terrorist organizations in the future.

With the support of the United States, the European Union, the Organization of Economic Cooperation and Development has begun a crackdown on tax havens by targeting 36 jurisdictions which it said participate in unfair tax competition and undermine other nations’ tax bases. The OECD approach does not punish countries just for having low tax rates, instead, it looks for tax systems that have a lack of transparency, a lack of effective exchange of information and those countries that have different tax rules for foreign investors than for its citizens. Countries with these types of tax systems assist terrorists and international criminal organizations looking to hide money that was derived from the sale of drugs, weapons and other criminal enterprises that have already been laundered in the international financial system.

Mr. President, earlier this evening my colleague Senator Feingold offered an amendment to the section of the USA Patriot Act that deals with the interception of computer trespass communications. This amendment, at its core, was intended to prevent law enforcement from abusing their authority to monitor computer activity. The Senator from Wisconsin’s amendment would have limited the amount of time that law enforcement could monitor suspicious activity without a court order to 96 hours, after which time investigators would have to obtain a warrant for continued surveillance. I support the intent of the Senator. Mr. President, I felt compelled vote to table the amendment. I voted to table the amendment for two reasons: First, I was concerned that the amendment was overly restrictive because it prevented law enforcement from investigations unrelated to the computer trespass. My concern is that law enforcement authorities would, for example, be able to monitor activity which permitted a law enforcement agency to establish a ‘dead drop’ zone for terrorists to post messages, but would not be able to monitor the content of those messages. I also voted to table Senator Feingold’s amendment because I strongly believe that we must move forward with this anti-terrorism legislation. Just today the FBI issued a statement warning of terrorist attacks and put law enforcement on the highest alert. I believe these serious threats to our security justify our this legislation swiftly. But I sincerely hope that an acceptable compromise can be reached—on this and on other issues—in the final legislation.

This legislation is a crucial step toward limiting the scourge of money laundering and to stop the development of international criminal organizations. It is my hope that the Congress will be able to develop anti-terrorism legislation that will provide the needed protections of our citizens without eliminating any of our cherished individual liberties. Ms. Snowe, Mr. President, in the war against terrorism, Americans stand as one behind our President. Now, in the all-out effort to protect our homeland, Federal agencies must be united in securing American soil.

In that light, President Bush made exactly the right decision when he created the Office of Homeland Security—a national imperative in the wake of the horrific tragedies of September 11—and I commend him for appointing my former colleague, Pennsylvania Governor Tom Ridge, as its director. With this amendment on the table, Governor Ridge will literally be at the President’s side, giving him the standing that will be required to remove jurisdictional hurdles among the forty-plus agencies he will be responsible for coordinating.

I saw firsthand the consequences of serious inadequacies in coordination and communication during my twelve years as ranking member of the House Foreign Affairs International Operations Subcommittee. As chair of the committee’s Senate counterpart. In conducting oversight of embassy security as well as visa and consular operations, I became extensively involved with the issue of terrorism, co-drafting anti-terrorism legislation with former Representative Dan Mica, Florida, in the wake of 1983 and 1984 terrorist attacks against the U.S. embassy and Marine barracks in Lebanon; traveling to Belgrade, Warsaw, and East Berlin to press government officials into helping law enforcement and the Attorney General of the United States to track down the terrorist Abu Nidal and his organization; and investigating entry into the United States by radical Egyptian cleric Sheikh Omar Abdel Rahman, mastermind of the World Trade Center bombing in 1993.

As far back as our hearings on the 1985 Inman Report, commissioned in response to the attacks in Lebanon, it was abundantly clear that improved coordination and consolidation of information from agencies such as the FBI, CIA, DEA, Customs, INS and the State Department would be an essential step toward removing a vulnerability in our national security. That point was tragically underscored by our discovery that, astoundingly, in the period since 1987 when Sheikh Rahman was placed on the State Department lookout list, the Sheikh entered and exited the U.S. five times totally unimpeded. Even after the State Department formally issued a certification of visa revocation, he was granted permanent residence status by the INS. When he was finally caught on July 31, 1991, reentering the United States, he was immediately released back into U.S. society to allow him to pursue a multi-year appeal process.

Just as unbelievable is the fact that, even after the 1993 attack on the World Trade Center, membership in a terrorist organization in and of itself with the exception of the PLO—was not sufficient grounds for visa denial. Rather, the Immigration Act of 1990 required the Government to prove that an individual either was personally involved in a terrorist act, or planning one. This absurd threshold made it almost impossible to block individuals, such as Sheikh Rahman, from entering the country legally. Legislation I introduced in 1993 removed that bureaucratic and legal obstacle—yet it took nearly 3 more years to enact it as part of the Anti-Terrorism and Effective Death Penalty Act of 1996.

Further, to respond to the trail of errors we uncovered, provisions from my bill were enacted in 1994 requiring modernization in the State Department’s antiquated microfiche “lookout” system to keep dangerous aliens from entering the United States. This system required manual searches, was difficult to use, and was subject to error. The language I crafted required State to replace the old systems with one of two forms of state-of-the-art computerized systems. Visa fees were even increased for non-immigrants to pay for the upgrade.

Recognizing the need to make these new technologies with the need for the most comprehensive, current and reliable information, we also attempted to address the issue of access. This was all the more pressing because, in 1990, the Justice Department had ruled that because the State Department was not a “law enforcement agency”, it no longer had free access to the FBI’s National Crime Information Center. This system, which maintains arrest and criminal records, is used by the Federal Bureau of Investigation and the Department of Justice, and the local authorities in the state, as well as by the FBI itself. The government had to pay fees to access the data, and agents had to spend a lot of time to get the information they needed.
after it lost access to the NCIC, the visa denial rate for past criminal activities plunged a remarkable 45 percent—stark evidence that we can’t afford to tie the hands of America’s overseas line of defense against terrorism.

In the aftermath of the terrorist attacks on the World Trade Center and the Pentagon, the attention of the American people has turned to the security of our national border system and how these attackers were able to exploit that system to plot these dastardly acts.

The September 11 attacks have highlighted numerous loopholes in our immigration laws that have allowed terrorists to enter the United States posing as students, tourists or business visitors. In some cases, by simply walking across an unpatrolled border. In reviewing our counter-terrorism efforts within our intelligence community, it is also appropriate that we look at the numerous immigration loopholes these terrorists were able to exploit.

There are currently between 7 million and 13 million illegal aliens living in the United States. Six out of 10 of these aliens crossed a U.S. border illegally, and therefore were not subject to background checks by the INS or the State Department to determine if they had a terrorist or criminal history. In fact, exit/entry records are so incomplete that the Immigration and Naturalization Service, INS, has no record of 6 of the 19 suspected hijackers entering the United States.

Of the roughly 10,000 INS agents guarding our borders, only 3 percent are stationed on our northern border with Canada. That’s 334 agents protecting our entire 12,000 mile border for one 12 miles. According to media reports, a number of the September 11 terrorists crossed this border to enter the United States. Of those foreign nationals who have legally entered the United States, more than a half-a-million of them are registered as international students at 15,000 universities, colleges, and vocational schools across the United States. These are nuclear engineering scholars, biochemistry students, and even pilot trainees who have access to dangerous technology, training, and information.

The Congress passed legislation in 1996 requiring the INS to create a database for international students. The purpose was to more efficiently monitor the immigration/visa status and whereabouts of students from abroad. After 5 years, there is still no system in place to monitor these 500,000 students. The current pilot program operating at 21 schools is not expected to be fully operational for five more years, and even that date could slip.

Without a monitoring system in place to audit schools that sponsor these students, there is nothing to prevent an alien from entering the United States on a student visa and then just disappearing. Consequently, one of the September 11 hijackers was able to enter the United States on a student visa, dropped out, and remained illegally thereafter.

Absuses of the visa system can also be found in the application process overseas at our U.S. consulates. Foreign nationals must apply for a visa at a U.S. consulate abroad and go through a series of security checks before they can enter the United States. Some media reports have raised the issue of consulate shopping, that is, foreign nationals choosing to apply at a U.S. consulate that they believe is most likely to grant them a visa. The “New York Times” reported in September that Chinese nationals applying for visas at a U.S. consulate in Beijing compare the experience to country in hopes of finding a U.S. consulate which would be less familiar with his background and more likely to award him a visa. One terrorist who was involved in the 1993 World Trade Center bombing was deputed a visa at U.S. consulate in Egypt, only to be awarded a visa by the U.S. consulate in Sudan.

And these are loopholes that exist only for those terrorists who would risk a background check by seeking a visa at a U.S. consulate. The United States allows 29 countries to participate in a visa-waiver program, which effectively allows the citizens of many European countries to bypass the initial screening process to enter the United States abroad by waiving the visa requirement. The Inspector General for both the State and Justice Department have raised the possibility that a foreign national could steal and counterfeit a visa-free passport to bypass the visa background check altogether.

The October 8 Wall Street Journal reported that some 1,067 visa-free passports have been stolen in recent months, presumably to be used for entry into the United States. In fact, one of the terrorists who plotted the bombing of the 1993 World Trade Center bombing was caught trying to slip through this loophole in 1992 when he tried to enter the United States using a visa-free Swedish passport. These are just some of the loopholes that terrorists are trying to exploit. To its credit, the Senate Judiciary Committee recognizes the problem.

The legislation drafted by the committee would triple the number of INS agents on our northern border. This is a worthwhile investment, and one that should be made. However, the security of our borders depends on more than just INS agents. The first line of defense against terrorists are our U.S. consulates abroad.

We must address the loopholes in the visa-waiver program that would allow a potential terrorist to enter the United States on a stolen passport. We must prevent consulate shopping. And, we must fully implement a system that can monitor foreign students.

The State and Justice Departments confirm that these are real security threats that must be addressed if we are to protect our borders from terrorists.

I have offered three amendments to address these concerns, which were accepted by the Judiciary Committee chair and ranking member into the manager’s package.
My first amendment would authorize the necessary funding so that the Justice Department could immediately put in place a tracking system that would require every university, college, and vocational school to submit a name, an address, an enrollment status, and previous addresses on each of the international students that these educational institutions sponsor. Such a database would be invaluable to law enforcement officials who may need to identify and locate a potential terrorist.

My second amendment would tighten the visa-waiver program by requiring that any country that participates in that program issue to its citizens within 2 years machine-readable passports that U.S. officials could scan into a "look out" system. This moves forward the original statutory deadline Congress agreed to last year by 4 years.

This amendment would also require the State Department to regularly audit the entries of those visa-free countries to ensure that countries that participate in this program have implemented sufficient safety precautions to prevent the counterfeiting and the theft of their passports.

My third amendment would require the State Department to review how it issues its visas to determine if consular shipping is a problem, and then require the Secretary of State to take the necessary steps to correct the problem. The State Department has the legislative authority it needs to fix this problem. It is now imperative that it use that authority.

My amendments are important steps toward closing down the loopholes in our immigration laws, and I look forward to working with my colleagues so that we may continue to tighten the security of national borders.

Mr. HATCH. Mr. President, three weeks ago, the President of the United States divided us with his address to this Congress and the American people—announced a war on terrorism. In that address, he asked Congress to provide our law enforcement community with the tools they need to wage that war effectively.

After several weeks of negotiations with the Chairman and the Administration, I am pleased we have come to the point where we can pass a bipartisan, measured bill that does just that.

Mr. President, each of us has, in different ways, had our lives touched by the awful events of September 11th. Each of us has, in the days since the attack, been shocked and appalled by the stories of heroism and self-sacrifice that have emerged from around the country in the wake of these terrible events.

As the President made clear in his address to the nation, we did not seek this war. This war was thrust upon us—thrust upon us by an unprovoked attack upon our civilian population in the very midst of our greatest cities. And just one month later, we could not have conceived that Monday, October 11th, 2001, we would be at war. It is true that, for years, some of us in this Congress, and around the country, have warned that there were powerful, well-financed individuals located throughout the United States dedicated to the destruction of our way of life. But, few of us could predict the horrific methods that these men would employ in an effort to destroy us and our democratic institutions.

On September 11th, all that changed. In the last few weeks, we have all come to acknowledge that we live in a different and more dangerous world than the world we thought we knew when we woke up on the morning of September 11th...

... A different world—not only because thousands of our countrymen are dead as a result of the September 11th attacks...

... But a different world, also, because of the threat that there remains an ongoing and serious threat to our way of life and, in fact, to our health and well-being as a society.

As has been reported in the national media, the investigation into the September 11th attacks has revealed there are terrorist cells that continue to operate actively among us. It is a chilling thought, but it is true.

The war to which we have collectively committed is a war unlike any we have ever fought. It is different because a substantial part of this war must be fought on our own soil. This is not a circumstance of our choosing. The enemy has brought the war to us.

But we must not flinch from acknowledging the fact that, because this is a different kind of war, it is a war that will require different kinds of weapons, and different kinds of tactics.

The Department of Justice, and its investigative components including the FBI, the INS, and the Border Patrol, will continue to have the principal responsibility for identifying and eradicating terrorist activity within our national borders. Our intelligence community must have access to critical information available to our law enforcement community.

Over the last several weeks, the Attorney General has made clear to us, in no uncertain terms, that he does not currently have adequate weapons to fight this war. Weeks ago, the Administration sent to Congress a legislative proposal that would give the Department of Justice and others in law enforcement the tools they need to be effective in tracking down and eliminating terrorist activity in this country.

Over the last several weeks, Senator LEAHY, other members of the Judiciary Committee, and I have undertaken a painstaking review of the anti-terrorism proposal submitted by the Administration. There have been several hearings on this legislation in the Senate, and many briefings by experts and advocates.

I would like to congratulate Senator LEAHY, in particular, for his thoroughness in reviewing this legislation and his many thoughtful comments and suggestions in our joint effort to ensure that the proposals adequately protect the constitutional liberties of all Americans.

Now, after weeks of fine-tuning, we have reached a final product that accommodates the concerns of each of the Senators who support this bill. The bipartisan bill that we vote on today respects the constitutional liberties of the American people, and, at the same time, does what people around America have been calling upon us to do—provide our law enforcement community the tools they need to keep us safe in our homes, in our travels, and in our places of business.

I would like to make a few comments regarding the process for this legislation. Although we have considered this in a more expedited manner than other legislation, my colleagues can be assured that this bill has received thorough consideration. First, the fact is that much of these proposals have been requested by the Department of Justice for years, and have languished in Congress for years because we have been unable to muster the collective political will to enact them into law.

I see no reason why these tools could not have prevented the attacks of September 11th. But, as the Attorney General has said, it is certain that without these tools, we did not stop the vicious acts of last month. I say to my colleagues, Mr. President, that these tools could help us now to track down the perpetrators—if they will help us in our continued pursuit of terrorist activities within our national borders—then we should not hesitate any further to pass these reforms into law. As long as these reforms are consistent with our Constitution—and they are—it is difficult to see why anyone would oppose their passage.

Furthermore, I would like to clearly dispel the myth that the reforms in this legislation somehow abridge the Constitutional freedoms enjoyed by law-abiding American citizens. Some press reports have portrayed this issue
as a choice between individual liberties on the one hand, and on the other hand, enhanced powers for our law enforcement institutions. This is a false dichotomy. We should all take comfort that the reforms in this bill are primarily directed at allowing law enforcement the tools to work more efficiently—in no case do they curtail the precious civil liberties protected by our Constitution. I want to assure my colleagues that we worked very hard over the past several weeks to ensure this legislation upholds all of the constitutional freedoms our citizens cherish. It does.

I would like to take a minute to explain briefly a few of the most important provisions of this critical legislation.

First, the legislation encourages information-sharing between various arms of the federal government. I believe most of our citizens would be shocked to learn that, even if certain government agencies had prior knowledge of the September 11th attacks, under many circumstances they would have been prohibited by law from sharing that information with the appropriate intelligence or national security authorities.

This legislation makes sure that, in the future, such information flows freely within the Federal government, so that it will be received by those responsible for protecting against terrorist attacks.

By making these reforms, we are rejecting the outdated Cold War paradigm that has prevented cooperation between our intelligence community and our law enforcement agencies. Current law does not adequately allow for such cooperation, artificially hampering our government's ability to identify and prevent acts of terrorism against our citizens.

In this new war, Mr. President, terrorists are a hybrid between domestic criminals and international agents. We must lower the barriers that discourage our law enforcement and intelligence agencies from working together to stop these terrorists. These hybrid criminals call for new, hybrid tools.

Second, this bill updates the laws relating to electronic surveillance. Electronic surveillance, conducted under the supervision of a federal judge, is one of the most powerful tools at the disposal of the enforcement community. It is simply a disgrace that we have not acted to modernize the laws currently on the books which govern such surveillance, laws that were enacted before the fax machine came into common usage, and well before the advent of cellular telephones, e-mail, and instant messaging. The Department of Justice has asked us for years to update these laws to reflect the new technologies, but there has always been a call to go slow, to seek more information, to provide further studies.

This is no hypothetical problem. We now know that e-mail, cellular telephones, and the Internet have been principal tools used by the terrorists to coordinate their atrocious activities. We need to pursue all solid investigative leads that exist right now that our law enforcement agents would be unable to pursue because they must continue to work within these outdated laws so that our law enforcement agencies can deal with the world as it is, rather than the world as it existed 20 years ago.

A good example of the way we are handicapping our law enforcement agencies relates to devices called "pen registers." Pen registers may be employed by the FBI, after obtaining a court order, to determine what telephone numbers are being dialed from a particular telephone. These devices are essential investigatory tools, which allow law enforcement agents to determine who is speaking to whom, within a criminal conspiracy.

The Supreme Court has held, in Smith v. Maryland, that the information obtained by pen register devices is not information that is subject to ANY constitutional protection. Unlike the content of your telephone conversation once your call is connected, the numbers you dial into your telephone are not private. Because you have no reasonable expectation that such numbers will be kept private, they are not protected under the Constitution. The Smith holding was cited with approval by the Supreme Court just earlier this year.

The legislation under consideration today would make clear what the federal courts have already ruled—that federal judges may grant pen register authority to the FBI to cover, not just telephones, but other more modern modes of communication such as e-mail or instant messaging. Let me make clear that the bill does not allow law enforcement to receive the content of your e-mails, but it does allow law enforcement to receive the addressing information to identify the computer or computers a suspect is using to further his criminal activity.

Importantly, reform of the pen register law does not allow—as has sometimes been misreported in the press—for law enforcement agents to view the content of any e-mail messages—not even the subject line of e-mails. In addition, this legislation we are about to vote upon makes it explicit that content can not be collected through such pen register orders.

This legislation also allows judges to enter pen register orders with nationwide scope. Nationwide jurisdiction for pen register orders makes common sense. It helps law enforcement agents efficiently identify communications facilities throughout the country, which greatly enhances the ability of law enforcement to identify quickly other members of a criminal organization, such as a terrorist cell that we update our intelligence community with the same authority to use pen register devices, under the auspices of the Foreign Intelligence Surveillance Act, that our law enforcement agents have when investigating criminal offenses. It simply makes sense to provide law enforcement with the same tools to catch terrorists that they did in the 1970s in connection with other criminal investigations, such as drug crimes or illegal gambling.

In addition to the pen register statute, this legislation updates other aspects of our wiretapping statutes. It is amazing that law enforcement agents do not currently have authority to seek wiretapping authority from a federal judge when investigating a terrorist offense. This legislation fixes that problem.

Moving on, I note that much has been made of the complex immigration provisions of this bill. I know Senators KENDY, Senator KYL, and I worked out a compromise that limits the provision.

I want to assure my colleagues that we have worked hard to address your concerns, and the concerns of the public. As with the other immigration provisions of this bill, we have made painstaking efforts to achieve this workable compromise.

Let me address some of the specific concerns. In response to the concern that the INS might detain a suspected terrorist indefinitely, Senator KENNEDY, Senator KYL, and I worked out a compromise that limits the provision.

Moreover, Senator LEAHY and I have also worked diligently to craft necessary language that will allow the deportation of those aliens who are representatives of organizations that endorse terrorist activity, those who provide material support to terrorist organizations. If we are to fight terrorism, we can not allow those who support terrorists to remain in our country. Also, I should note that we have worked hard to provide the State Department and the INS the tools they need to ensure that no applicant for admission who is a terrorist is able to secure entry into the United States through legal channels.

Finally, the bill gives law enforcement agencies powerful tools to attack the financial infrastructure of terrorism—giving our government the ability to choke off the financing that these dangerous terrorist organizations need to survive. It also removes the practice of harboring terrorists, and puts teeth in the laws against providing material support to terrorists.
and terrorist organizations. It gives the President expanded authority to freeze the assets of terrorists and terrorist organizations, and provides for the eventual seizure of such assets. These tools are vital to our ability to effectively wage against terrorism, and ultimately to win it.

Mr. President, before this debate comes to an end, I would be remiss if I did not acknowledge the hard work put in by my staff, the staff of Senator Leahy, Senators Kyl, Specter, Durbin, and Leah Belaire, who have provided invaluable expertise to this process. My immigration counsel, Dustin Pead and my legislative assistant Brigham Cannon have been instrumental in putting this bill together. I also would like to thank my criminal counsel, Jeff Taylor, Stuart Nash and Leah Belaire, who have brought invaluable expertise to this process. My immigration counsel, Dustin Pead and my legislative assistant Brigham Cannon have provided invaluable assistance.

I would like to thank the staff of Senator LEAHY—his chief counsel Bruce Cohen, and other members of his staff—Beryl Howell, Julie Katzman, Ed Pagano, David James, and John Eliff.

The Department of Justice has been of great assistance to us in putting this bill together. I would like to thank Attorney General Ashcroft and his Deputy for their wise guidance and their quick response to our many questions and concerns. Michael Chertoff, the Assistant Attorney General for the Criminal Division was a frequent participant in our meetings, as well as Assistant Attorneys General Dan Bryant and Viet Dinh. Jennifer Newstead, John Yew, John Elwood and Pat O'Brien were all important participants in this process.

Finally, the White House staff provided essential contributions at all stages of this process. Judge Al Gonzales, the White House counsel provided key guidance, with the help of his wonderful staff, including Tim Flanagan, Courtney Elwood, and Porad Berenson.

In addition, members of the White House Congressional Liaison Office kept this process moving forward. I would like to thank Heather Wingate, Candace midnight Dorn for all the assistance they have given us.

There have been few, if any, times in our nation's great history where an event has brought home to so many of our citizens, so quickly, and in such a graphic fashion, of our vulnerability to unexpected attack.

I believe we all took some comfort when President Bush promised us that our law enforcement institutions would have the tools necessary to protect us from the danger that we are only just beginning to perceive.

The Attorney General has told us what tools he needs. We have taken the time to review the problems with our current laws, and to reflect on their solutions. The time to act is now. Let us please move forward expeditiously, and give those who are in the business of protecting us the tools that they need to do their jobs.

Mr. President, I urge my colleagues' support for this important legislation and yield the floor.

Mr. DASCHLE. Mr. President, 4 days ago, our military launched strikes against terrorist training camps and the Taliban's military installations in Afghanistan. They are intended to disrupt the network of terror that spreads across Afghanistan.

But these strikes are only a part of a much larger battle. The network that we seek to disrupt and ultimately destroy often operates without borders or boundaries. Its tools are not simply the weapons it chooses to employ. And its trails are more often electronic than physical.

This is a new kind of battle. Winning it will require a new set of tools . . . And winning is the only acceptable outcome.

Just as we are committed to giving our men and women in uniform the tools and training they need to do what is asked of them, we must now make that same commitment to our justice and law enforcement officials.

And winning is the only acceptable outcome.

I also want to thank the many other Democratic and Republican Senators whose insights and suggestions improved this legislation.

For example, Senator KENNEDY's input on provisions regarding immigration addressed concerns a number of us had about the detention of legal permanent residents with only few due process protections. And Senators ENZI, LEAHY and DORGAN were able to improve a provision regarding unilateral food and medical sanctions in a way that avoids needlessly hurting American farmers.

I'll be honest: this bill is not perfect, and I hope that we will be able to work with our House colleagues in the days ahead in order to improve it.

Whenever we weigh civil liberties versus national security, we need to do so with the utmost care. Among other things, I am concerned about the provisions within this bill that allow the sharing of information gathered in grand juries and through wiretaps without judicial check. And, as we give the administration new legitimate powers to wiretap under the Foreign Intelligence Surveillance Act, we should do more to protect the rights of Americans who are not suspects or targets of investigations.

These flaws are not insubstantial, but ultimately the need for this bill outweighs them. When it comes to an issue as central to our democracy as the protection of our people, we must act.

This bill does several important things:

First, it will enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance and execute searches in order to gather critical information to fight terrorism.

Second, it will permit broader information sharing between traditional law enforcement and foreign intelligence officers.

Third, it will increase the Attorney General's ability to deport and detain individuals who support terrorist activity. I should note, though, that the Senate bill requires the Attorney General either to bring criminal or immigration charges within seven days after taking custody of an alien or relinquish custody.

Fourth, this bill also takes significant steps to increase law enforcement presence on our northern border. For example, it would triple the number of Border Patrol, Customs Service, and INS inspectors at the northern border, who would work in concert with their Canadian counterparts in order to enhance security in this previously understaffed area.

Fifth, thanks in large part to Senator LEAHY's hard work, this bill makes major revisions to the Victims of Crime Act—by strengthening the Crime Victim Fund and expediting assistance to victims of domestic terrorism.

Sixth and finally, the Banking Committee was able to agree on, and add to this bill, several significant counter money laundering measures. If we are to truly fight terrorism on all fronts, we must fight it on the financial front as well.

As you can see, this is a complex piece of legislation. But its aim is simple: to give law enforcement the tools it needs to fight terrorism.

It was a month ago on this day that we suffered the worst terrorist attack in our Nation's history. In the days since, we have honored the memories of the more than 6,000 innocent men and women who lost their lives on that terrible day.

Hours ago, for example, we passed a resolution that designates September 11 as a national day of remembrance.

But I believe that to truly honor those whose lives were lost, we must match our words with action, and do all that we can in order to prevent future attacks.
This bill is a significant step towards keeping that commitment, and keeping Americans safe.

Mr. DASCHEL. It is my understanding that the managers intend now to yield back the remainder of the time on the bill and we will go straight to final passage.

First, I thank all Senators for their cooperation tonight. This was a very good day. We got a lot of work done, and I appreciate the work of all Members. There will not be rollcall votes tomorrow. In fact, we will not be in session. We will come in on Monday, midafternoon. There will be a vote on the motion to proceed to the foreign operations bill and a vote on the conference report to the Interior appropriations bill at approximately 5:30 Monday afternoon. I thank all Senators.

I yield the floor.

Mr. LEAHY. Mr. President, we are about to vote on final passage. We thought there would be a managers’ package. We signed off on this side, and apparently the other side has not, which is their right.

Mr. HATCH. We have a managers’ package. It is done. It is just being assembled and put together and will be here.

I yield the floor.

Mr. LEAHY. I am glad there will be a managers’ package. We cannot vote on final passage until the managers’ package is here. I thank the majority leader for his help. As I said before, I don’t think the bill could have gotten as far as it did without that help. I wish the administration had kept to the agreement they made September 30. We would have a more balanced bill. I still am not sure why the administration backed away from their agreement. I am the old style Vermonter: When you give an agreement, you stick with it. But they decided not to, and it slowed us up a bit.

The PRESIDING OFFICER. Let’s have order in the Senate Chamber so the Senator can be heard.

Mr. LEAHY. I yield the floor.

Mr. DASCHEL. Mr. President, I ask unanimous consent that notwithstanding the passage of the amendment, the managers’ amendment be considered subject to approval by both managers and both leaders.

The PRESIDING OFFICER. Is there objection?

Mr. BYRD. What is the request?

Mr. DASCHEL. Mr. President, I will repeat the request. There is a technical amendment having to do with some of the issues that have been worked out, that have no substantive consequence. I ask unanimous consent that this managers’ amendment be approved, notwithstanding the passage of the bill subject to approval by the two managers and the two leaders.

Mr. BYRD. Mr. President, I object to that.

The PRESIDING OFFICER. Objection is heard.

Mr. BYRD. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. LEAHY. Mr. President, I ask unanimous consent the order for the quorum call be dispensed with.

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

Mr. LEAHY. I yield all time. I ask for the yeas and nays on final passage.

The PRESIDING OFFICER. The Senator from Vermont is recognized.

Mr. LEAHY. I ask for the yeas and nays on final passage.

The PRESIDING OFFICER. Is there a sufficient second?

There is a sufficient second.

The yeas and nays were ordered.

The PRESIDING OFFICER. The clerk will read the bill for the third time.

Mr. FEINGOLD. Mr. President, what is the status?

The PRESIDING OFFICER. The bill is ready for third reading.

Mr. FEINGOLD. I ask the Chair if the managers’ amendment has been adopted.

The PRESIDING OFFICER. It has not.

Mr. FEINGOLD. I thank the Chair.

The PRESIDING OFFICER. There has been none submitted.

The question is on the engrossment and third reading of the bill.

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

The PRESIDING OFFICER. The bill having been read the third time, the question is, Shall the bill pass?

The yeas and nays have been ordered.

The clerk will call the roll.

The legislative clerk called the roll.

Mr. NICKLES. I announce that the Senator from North Carolina (Mr. HELMS), the Senator from South Carolina (Mr. THURMOND), and the Senator from New Mexico (Mr. DOMENICI) are necessarily absent.

I further announce that if present and voting the Senator from North Carolina (Mr. HELMS) would vote ‘yea.’

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 96, nays 1, as follows:

[Rollcall Vote No. 302 Leg.]

<table>
<thead>
<tr>
<th>Yeas 96</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akaka</td>
</tr>
<tr>
<td>Allard</td>
</tr>
<tr>
<td>Allen</td>
</tr>
<tr>
<td>Baucus</td>
</tr>
<tr>
<td>Bayh</td>
</tr>
<tr>
<td>Bennett</td>
</tr>
<tr>
<td>Biden</td>
</tr>
<tr>
<td>Bingaman</td>
</tr>
<tr>
<td>Bond</td>
</tr>
<tr>
<td>Bunning</td>
</tr>
<tr>
<td>Burns</td>
</tr>
<tr>
<td>Byrd</td>
</tr>
<tr>
<td>Campbell</td>
</tr>
<tr>
<td>Cantwell</td>
</tr>
<tr>
<td>Carper</td>
</tr>
</tbody>
</table>

Yeas: Akaka, Allard, Allen, Baucus, Bayh, Bennett, Biden, Bingaman, Bingaman, Bond, Bunning, Burns, Byrd, Campbell, Cantwell, Carper

Nays: Corzine

The PRESIDING OFFICER. The bill (S. 1510) as passed as follows:

S. 1510

SECTION I. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Uniting and Strengthening America Act” or the “USA Act of 2001.”

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

Sec. 1. Short title and table of contents.

Sec. 2. Construction; intergovernmental cooperation.

TITLE I—ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 101. Counterterrorism fund.

Sec. 102. Sense of Congress condemning discrimination against Arab and Muslim Americans.

Sec. 103. Increased funding for the technical support center at the Federal Bureau of Investigation.

Sec. 104. Requests for military assistance to enforce prohibition in certain emergencies.

Sec. 105. Expansion of national electronic crime task force initiative.

Sec. 106. Presidential authority.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.

Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

Sec. 203. Authority to share criminal investigative information.

Sec. 204. Clarification of intelligence exceptions from communications interception and disclosure of wire, oral, and electronic communications.

Sec. 205. Employment of translators by the Federal Bureau of Investigation.

Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

Sec. 208. Designation of judges.

Sec. 209. Seizure of voice-mail messages pursuant to warrants.


Sec. 211. Clarification of scope.

Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

Sec. 213. Authority for delaying notice of the execution of a warrant.

Sec. 214. Pen register and trap and trace authority under FISA.

Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.
Sec. 211. Modification of authorities relating to the use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications.

Sec. 218. Foreign intelligence information.

Sec. 219. Single-jurisdiction search warrants for terrorism.

Sec. 220. Nationwide service of search warrants for electronic evidence.

Sec. 221. Trade sanctions.

Sec. 222. Assistance to law enforcement agencies.

Sec. 336. Bank Secrecy Act advisory group.

Sec. 335. Authorization to include suspicions.

Sec. 334. Anti-money laundering strategy.

Sec. 333. Penalties for violations of geo-

Sec. 332. Anti-money laundering programs.

Sec. 331. Amendments relating to reporting.

SUBTITLE B—INTERNATIONAL COUNTER MONEY LAUNDERING AND RELATED MEASURES

Sec. 311. Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern.

Sec. 312. Special due diligence for correspondent accounts and primary money laundering.

Sec. 313. Exclusion of aliens involved in financial shell banks.

Sec. 314. Cooperatives efforts to deter money laundering.

Sec. 315. Inclusion of foreign corruption offenses as money laundering crimes.

Sec. 316. Anti-terrorist forfeiture protection.

Sec. 317. Long-arm jurisdiction over foreign money launderers.

Sec. 318. Laundering money through a foreign bank.

Sec. 319. forfeiture of funds in United States interbank accounts.

Sec. 320. Proceeds of foreign crimes.

Sec. 321. Exclusion of aliens involved in money laundering.

Sec. 322. Corporation represented by a fugitive.

Sec. 323. Enforcement of foreign judgments.

Sec. 324. Increase in civil and criminal penalties for money laundering.

Sec. 325. Report and recommendation.

Sec. 326. Report on effectiveness.

Sec. 327. Concentration accounts at financial institutions.

SUBTITLE B—CURRENCY TRANSACTION REPORTING AMENDMENTS AND RELATED IMPROVEMENTS

Sec. 331. Amendments relating to reporting of suspicious activities.

Sec. 332. Anti-money laundering programs.

Sec. 333. Penalties for violations of geographic targeting orders and certain recordkeeping requirements, and lengthening effective period of geographic targeting orders.

Sec. 334. Anti-money laundering strategy.

Sec. 335. Authorization to include suspicious of illegal activity in written examination references.

Sec. 336. Bank Secrecy Act advisory group.

Sec. 337. Agency reports on reconciling penalty amounts.

Sec. 338. Reporting of suspicious activities by securities brokers and dealers.

Sec. 339. Special report on administration of Bank Secrecy provisions.

Sec. 340. Bank Secrecy provisions and anti-terrorist activities of United States intelligence agencies.

Sec. 341. Reporting of suspicious activities by hawala and other underground banking systems.

Sec. 342. Use of Authority of the United States Executive Directors.

SUBTITLE D—CURRENCY CRIMES

Sec. 351. Bulk cash smuggling.

SUBTITLE E—ANTICORRUPTION MEASURES

Sec. 361. Corruption of foreign governments and elite.

Sec. 362. Support for the financial action task force on money launderers.

Sec. 363. Terrorist funding through money laundering.

TITLE IV—PROTECTING THE BORDER

Sec. 401. Ensuring adequate personnel on the Border.

Sec. 402. Northern border personnel.

Sec. 403. Access by the Department of State and the INS to certain identifying information in the criminal history records of visa applicants and applicants for admission to the United States.

Sec. 404. Limited authority to pay overtime.

Sec. 405. Report on the integrated automated fingerprint identification system for points of entry and overseas consular posts.

Sec. 411. Definition relating to terrorism.

Sec. 412. Mandatory detention of suspected terrorists; habeas corpus; judicial review.

Sec. 413. Multilateral cooperation against terrorists.

TITLE V—REMOVING OBSTACLES TO INVESTIGATING TERRORISM


Sec. 502. Attorney General’s authority to pay rewards to combat terrorism.

Sec. 503. Secretary of State’s authority to pay rewards.

Sec. 504. DNA identification of terrorists and other violent offenders.

Sec. 505. Coordination with law enforcement.

Sec. 506. Miscellaneous national security authorities.

Sec. 507. Extension of Secret Service jurisdiction.

Sec. 508. Disclosure of educational records.

Sec. 509. Disclosure of information from NCIS surveys.

TITLE VI—PROVIDING FOR VICTIMS OF TERRORISM, PUBLIC SAFETY OFFICERS, AND THEIR FAMILIES

Sec. 601. Aid to Families of Public Safety Officers.

Sec. 602. Expanded payment for public safety officers involved in the prevention, investigation, rescue, or recovery efforts related to a terrorist attack.

Sec. 603. Technical correction with respect to expedited payments for heroic public safety officers.

Sec. 604. Public Safety Officers Benefit Program payment increase.

Sec. 605. Office of Justice programs.


Sec. 607. Crime Victims Fund.

Sec. 608. Crime victim compensation.

Sec. 609. Crime victim assistance.

Sec. 610. Victims of terrorism.

TITLE VII—STRENGTHENING THE INTELLIGENCE COMMUNITY

Sec. 701. Material support for terrorism.

Sec. 702. Jurisdiction over crimes committed at U.S. facilities abroad.

Sec. 703. Material support for terrorism.

Sec. 704. Assets of terrorist organizations.

Sec. 705. Technical clarification relating to provision of material support to terrorists.

Sec. 706. Definition of Federal crime of terror.

Sec. 711. No statute of limitation for certain terrorism offenses.

Sec. 712. Alternate maximum penalties for terrorism offenses.

Sec. 713.Penalties for terrorist conspiracies.

Sec. 714. Post-release supervision of terrorists.

Sec. 715. Inclusion of acts of terrorism as racketeering activity.

Sec. 716. Deterrence and prevention of cyberterrorism.

Sec. 717. Additional defense to civil actions relating to preserving records in response to government requests.

Sec. 718. Development and support of cybersecurity forensic capabilities.

TITLE VII—ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 801. Responsibilities of Director of Central Intelligence regarding foreign intelligence collected under Foreign Intelligence Surveillance Act of 1978.

Sec. 802. Inclusion of international terrorist activities within scope of foreign intelligence, under National Security Act of 1947.

Sec. 803. Sense of Congress on the establishment and maintenance of intelligence relationships to acquire information on terrorists and terrorist organizations.

Sec. 804. Temporary authority to defer submittal to Congress of reports on intelligence and intelligence-related matters.

Sec. 805. Disclosure to director of central intelligence of foreign intelligence-related information with respect to criminal investigations.

Sec. 806. Foreign terrorist asset tracking center.

Sec. 807. National virtual translation center.

Sec. 808. Training of government officials regarding identification and use of foreign intelligence.

SECT. 2. CONSTRUCTION; SEVERABILITY.

Any provision of this Act held to be invalid or unenforceable by its application to any person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this Act and shall not affect the remainder thereof or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

TITLE VIII—STRENGTHENING THE CRIMINAL LAWS AGAINST TERRORISM

Sec. 901. Terrorist attacks and other acts of violence against mass transportation systems.

Sec. 902. Expansion of the biological weapons statute.

Sec. 903. Definition of domestic terrorism.

Sec. 904. Prohibition against harboring terrorists.

Sec. 905.Jurisdiction over crimes committed at U.S. facilities abroad.

Sec. 906. Material support for terrorism.

Sec. 907. Assets of terrorist organizations.

Sec. 908. Technical clarification relating to provision of material support to terrorist.

Sec. 909. Definition of Federal crime of terrorism.

Sec. 910. No statute of limitation for certain terrorism offenses.

Sec. 911. Alternate maximum penalties for terrorism offenses.

Sec. 912. Penalties for terrorist conspiracies.

Sec. 913. Post-release supervision of terrorists.

Sec. 914. Inclusion of acts of terrorism as racketeering activity.

Sec. 915. Deterrence and prevention of cyberterrorism.

Sec. 916. Additional defense to civil actions relating to preserving records in response to government requests.

Sec. 917. Development and support of cybersecurity forensic capabilities.
the “Counterterrorism Fund”, amounts in which shall remain available without fiscal year limitation—
(1) to reimburse any Department of Justice component for any costs incurred in connection with—
(A) reestablishing the operational capability of an office or facility that has been damaged or destroyed as the result of any domestic or international terrorism incident;
(B) providing support to counter, investigate, or prosecute domestic or international terrorism, including, without limitation, paying rewards in connection with these activities; and
(C) conducting terrorism threat assessments of Federal agencies and their facilities;
(2) to reimburse any department or agency of the Federal Government for any costs incurred in connection with detaining in foreign countries individuals accused of acts of terrorism that violate the laws of the United States.

(b) No EFFECT ON PRIOR APPROPRIATIONS.—
Subsection (a) shall not be construed to affect the validity or availability of any appropriation to the Counterterrorism Fund made before the date of enactment of this Act.

SEC. 102. SENSE OF CONGRESS CONDEMNING DISCRIMINATION AGAINST ARAB AND MUSLIM AMERICANS. (a) FINDINGS.—Congress makes the following findings:
(1) Arab Americans, Muslim Americans, and Americans from South Asia play a vital role in our Nation and are entitled to nothing less than the full rights of every American.
(2) The acts of violence that have been taken against Arab and Muslim Americans since the September 11, 2001, attacks against the United States and the people and the homeland of the Arab and Muslim Americans, and the Jewish Americans, and all Americans who value freedom.
(3) The concept of individual responsibility for wrongdoing is sacrosanct in American society, and applies equally to all religious, racial, and ethnic groups.
(4) When American citizens commit acts of violence against those who are, or are perceived to be, of Arab or Muslim descent, they should be punished to the full extent of the law.
(5) Muslim Americans have become so fearful of harassment that many Muslim women are changing the way they dress to avoid becoming targets.
(6) Muslim Americans and Muslim Americans have acted heroically during the attacks on the United States, including Mohammed Salim Hamdani, a 23-year-old New Yorker of Pakistani descent, who is believed to have gone to the World Trade Center to offer rescue assistance and is now missing.
(b) SENSE OF CONGRESS.—It is the sense of Congress that—
(1) the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, are protected, and that every effort must be taken to preserve their safety;
(2) any acts of violence or discrimination against any Americans be condemned; and
(3) the Nation is called upon to recognize the patriotism of fellow citizens from all ethnic, racial, and religious backgrounds.

SEC. 103. INCREASED FUNDING FOR THE TECHNICAL SUPPORT CENTER AT THE FEDERAL BUREAU OF INVESTIGATION. There are authorized to be appropriated for the Technical Support Center established in section 811 of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 110 Stat. 1294) to help meet the demands and activities to combat terrorism and support and enhance the technical support and tactical operations of the FBI, $230,000,000 for each of the fiscal years 2002, 2003, and 2004.

SEC. 104. REQUESTS FOR MILITARY ASSISTANCE TO THE UNITED STATES SECRET SERVICE IN CERTAIN EMERGENCIES. Section 2332e of title 18, United States Code, is amended—
(1) by striking “2332c” and inserting “2332a”; and
(2) by striking “chemical”.

SEC. 105. EXPANSION OF NATIONAL ELECTRONIC CRIMES TASK FORCE INITIATIVE. The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, to be known as the Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

SEC. 106. PRESIDENTIAL AUTHORITY. Section 203 of the International Emergency Powers Act (50 U.S.C. 1702) is amended—
(1) in subsection (a)—
(A) at the end of subparagraph (A) (flush to that subparagraph), by striking “; and” and inserting a comma and the following: “by any person, or with respect to any property, subject to the jurisdiction of the United States;”;
(B) in subparagraph (B)—
(i) by inserting “; block during the pendency of an investigation” after “investigate”; and
(ii) by striking “interest;” and inserting “interest by any person, or with respect to any property, subject to the jurisdiction of the United States;” and;
(C) by inserting at the end the following:
“(C) when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States; and all right, title, and interest in any property so confiscated shall vest, when, as, and upon the terms directed by the President, in such agency or person on the President as the President may designate. In this subparagraph and upon such terms and conditions as the President may prescribe, such interest or property shall be held, used, administered, liquidated, sold, or otherwise dealt with in the interest of and for the benefit of the United States, and such designated agency or person may perform any and all acts incident to the accomplishment or furtherance of these purposes.;” and
(2) by inserting at the end the following:
“(C) CLASSIFIED INFORMATION.—In any judicial review of a determination made under section 206(b) of the Act, information was based on classified information (as defined in section (a) of the Classified Information Procedures Act) submitted to the reviewing court ex parte and in camera. This subsection does not confer or imply any right to judicial review.”.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM. Section 2516(1) of title 18, United States Code, is amended—
(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 110 Stat. 1294), as subsection (p); and
(2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104–208; 110 Stat. 3009–565), the following new paragraph:
“Any criminal violation of section 229 (relating to chemical weapons); or sections 2322, 2322a, 2322b, 2324a, or 2329B of this title (relating to terrorism) or;

SEC. 202. AUTHORITY TO SHARE ELECTRONIC WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES. Section 2518(1)(c) of title 18, United States Code, is amended by striking “section 1341 (relating to mail fraud),” and inserting “section 1341 (relating to mail fraud), a felony violation of section 1029 (relating to computer fraud and abuse offense),”.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION. (a) AUTHORITY TO SHARE GRAND JURY INFORMATION.—
(1) IN GENERAL.—Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended—
(A) in clause (III), by striking “or” at the end;
(B) in clause (IV), by striking the period at the end and inserting “; and”;
(C) by inserting at the end the following:
“(v) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 403));”.

(2) DEFINITION.—Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure, as amended by paragraph (1), is amended by—
(A) inserting “(v)” after “(C)”;
(B) redesignating clauses (i) through (v) as subclauses (I) through (IV), respectively; and
(C) inserting at the end the following:
“(IV) information, whether or not concerning a United States person, that relates to the national defense or the security of the United States; or
(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(aa) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—
(bb) the conduct of the foreign affairs of the United States; or
(bb) the conduct of the foreign affairs of the United States;”.
(b) AUTHORITY TO SHARE ELECTRONIC WIRE, ORAL, AND ELECTRONIC INTERCEPTION INFORMATION.—
(1) LAW ENFORCEMENT.—Section 2518 of title 18, United States Code, is amended by inserting at the end the following:
“(vii) any investigative or law enforcement officer, or attorney for the Government, who has obtained knowledge of the contents of any wire, oral, or electronic communication, or
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power;

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;

(iv) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(b) Training and translators.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.

(d) Foreign Intelligence information.—

(1) General.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to protect the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this subsection shall assure that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition.—In this subsection, the term “foreign intelligence information” means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; or

(ii) espionage or intelligence activities by a foreign intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.

(d) Foreign Intelligence information.—

(1) General.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to protect the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this subsection shall assure that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition.—In this subsection, the term “foreign intelligence information” means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; or

(ii) espionage or intelligence activities by a foreign intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.

(d) Foreign Intelligence information.—

(1) General.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to protect the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this subsection shall assure that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition.—In this subsection, the term “foreign intelligence information” means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; and

(ii) espionage or intelligence activities by a foreign intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.

(d) Foreign Intelligence information.—

(1) General.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to protect the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this subsection shall assure that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition.—In this subsection, the term “foreign intelligence information” means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; and

(ii) espionage or intelligence activities by a foreign intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2516(1) and Rule 6(e)(3)(C)(v) of the Federal Rules of Criminal Procedure that identifies a United States person; and coordinates with the FBI and other components of the Department of Justice the needs of the FBI for specific translators to support counterterrorism investigations or for 120 days, whichever is less.
SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT AGAINST TERRORISM.

(a) Disclosure of Contents.—

(1) In general.—Section 2702 of title 18, United States Code, is amended—

(A) by striking the section heading and inserting the following:

"§ 2702. Voluntary disclosure of customer communications or records;"

(B) in subsection (a)—

(i) in paragraph (2)(A), by striking "and" and "them" and inserting "or"; and

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

"(C) a provider of remote computing service or a provider of electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity;"

(C) in subsection (b), by striking "EXCEPTIONS.—A provider described in subsection (a) may divulge a record or other information to a governmental entity to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity;"

(D) in subsection (b), by striking "EXCEPTIONS.—A provider described in subsection (a) may divulge a record or other information to a governmental entity to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity;"

(E) by inserting after subparagraph (C) as paragraph (2);

(iv) by designating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (A) as redesignated by striking the period and inserting "; or;"

(with respect to the issuance of a warrant to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

"(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);"

"(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communications covering the contents of communications, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

"(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown."

SEC. 214. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended—

(1) by inserting "(a) IN GENERAL.—" before "in addition"; and

(2) by adding at the end the following:

"(b) DELAY.—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

"(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);"

"(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communications covering the contents of communications, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

"(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown."
protected by the first amendment to the Constitution.

“(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

“(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a); or

(B) the United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

“(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

“(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

“(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

“SEC. 592. CONGRESSIONAL OVERSIGHT.

“(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

“(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

(2) the total number of such orders either granted, modified, or denied.

“SEC. 216. MODIFICATION OF AUTHORITY RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS.—Section 3122(c) of title 18, United States Code, is amended—

(1) by inserting “or trap and trace device” after “pen register”;

(2) by inserting “ routing, addressing,” after “dialing”; and

(3) by striking “calling process” and inserting “the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications”;

(b) ISSUANCE OF ORDERS.—Section 3123(a) of title 18, United States Code, is amended to read as follows:

“(a) IN GENERAL.—

“(1) ATTORNEY FOR THE GOVERNMENT.—

Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has the certificate of the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall be served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

“(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—Upon an application and under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device for a period of time not to exceed 90 days for an investigation of the phone line to which the pen register or trap and trace device is to be attached or applied, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(3), the geographic limits of the order; and

(3) NONDISCLOSURE REQUIREMENTS.—Section 3122(b)(1) of title 18, United States Code, is amended—

(A) in subparagraph (A),—

(i) by inserting “or other facility” after “telephone line”; and

(ii) by inserting before the semicolon at the end “or applied”; and

(B) by striking subparagraph (C) and inserting the following:

“(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and

(4) CONTENTS OF ORDER.—Section 3123(b)(1) of title 18, United States Code, is amended—

(A) by inserting “or other facility” after “the line”; and

(B) by striking “or who has been ordered by the court” and inserting “or applied, or who is obligated by the order”.

(c) DEFINITIONS.—

(1) COURT OF COMPETENT JURISDICTION.—Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

“(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having exclusive jurisdiction over the offense being investigated; or

(2) PEN REGISTER.—Section 3127(3) of title 18, United States Code, is amended—

(A) by striking “any other impulsive” and all that follows through “is attached” and inserting “dialing, routing, addressing, or signaling information transmitted or applied, or other information transmitted or applied, or a device” and inserting “or process” after “device” each place it appears.

“(3) TRAP AND TRACE DEVICE.—Section 3127(4) of title 18, United States Code, is amended—

(A) by striking of an instrument” and all that follows through the semicolon and inserting “or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, and, however, that such information shall not include the contents of any communication”; and

(B) by inserting “or process” after “a device”.

“(4) CONFORMING AMENDMENT.—Section 3127(1) of title 18, United States Code, is amended—

(A) by striking “and” and

(B) by inserting “, and contents” after “electronic communication service.”

“51. TECHNICAL AMENDMENT.—Section 3124(d) of title 18, United States Code, is amended by striking “the terms of”.

“SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

Chapter 119 of title 18, United States Code, is amended—

(1) in section 2510—

(A) in paragraph (17), by striking “and” at the end,

(B) in paragraph (18), by striking the period and inserting after paragraph (18) the following:

“(19) ‘protected computer’ has the meaning set forth in section 1030; and

“(20) ‘computer trespasser’ means

“(A) a means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

“(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer;” and

(2) in section 2511(2), by inserting at the end the following:

“(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser, if—

“(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer,

“(II) the person acting under color of law is lawfully engaged in an investigation,

“(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation; and

“(IV) such interception does not interfere communications other than those transmitted to or from the computer trespasser”.

“SEC. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 103(a)(7)(B) and 305(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking ‘‘the purpose’’ and inserting ‘‘a significant purpose’’.

“SEC. 219. SINGLE-JURISDICTION SEARCH WARRANTS FOR DOMESTIC OR INTERNATIONAL TERRORISM.

Rule 41(a) of the Federal Rules of Criminal Procedure is amended by inserting after ‘‘executed’’ the following: ‘‘and (3) in an investigation of domestic or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which an authorization to conduct a search is related to the terrorism, for a search of property or for a person within or outside the district.’’
TITLE III—INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

SEC. 201. SHORT TITLE.
This title may be cited as the “International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001”.

SEC. 202. FINDINGS AND PURPOSES.
(a) Findings—The Congress finds that—
(1) money laundering, estimated by the International Monetary Fund to amount to between 2 and 5 percent of global gross domestic product, and involving the flow of at least $600,000,000,000 annually, provides the financial fuel that permits transnational criminal enterprises to conduct and expand their operations to threaten the safety and security of American citizens;
(2) money laundering, and the defects in financial transparency on which money launderers rely, are critical to the financing of global terrorism and the provision of funds for terrorist attacks;
(3) money launderers subvert legitimate financial mechanisms and regimes through their close relationships with them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism, and, by doing so, can evade criminal, money laundering, and anti-money laundering regimes of both the United States and other States, and launder proceeds derived from violations of United States foreign and domestic laws, including Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and title 18, United States Code, sections 1961-1968, 510, 1555(a) and (b), 1556, and 1563(c), 26 U.S.C. 7203; 8 U.S.C. 1182(a)(3); 19 U.S.C. 1337; 22 U.S.C. 4081(a); 50 U.S.C. 2101a; 12 U.S.C. 218a; 26 U.S.C. 7301, 7345(a); 4120, 4121, 4122, 4123; 28 U.S.C. 523(a)(3); any foreign law or regulation, or other requirement for its involvement in international transactions that pose particular, identifiable opportunities for criminal abuse;
(4) to ensure that the forfeiture of any assets that are of particular, identifiable opportunities for criminal abuse;
(5) to strengthen the provisions put into place by the Money Laundering Control Act of 1986 (18 U.S.C. 981 note) and the International Money Laundering Act of 1994, and to provide a clear national mandate for subjecting to special scrutiny those financial institutions, financial institutions operating outside of the United States, and classes of international transactions that pose particular, identifiable opportunities for criminal abuse;
(6) to provide guidance to domestic financial institutions operating outside of the United States, and classes of international transactions that are of particular, identifiable opportunities for criminal abuse;
(7) to ensure that the forfeiture of any assets in connection with the anti-terrorism efforts of the United States permits for adequate challenge consistent with providing due process rights;
(8) to clarify the terms of the safe harbor from civil liability for filing suspicious activity reports;
(9) to strengthen the authority of the Secretary to issue geographic targeting orders, and to clarify that violations of such orders or any other requirements imposed under the authority contained in chapter 2 of title I of Public Law 91-508 and chapters II and III of title 31, United States Code, may result in criminal and civil penalties;
(10) to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities, and that jurisdictional disputes do not hinder examination of such transactions by financial institutions with relevant reporting requirements;
(11) to fix responsibility for high level coordination of the anti-money laundering efforts of the Department of the Treasury;
(12) to provide additional international anti-money laundering principles and recommendations.
(b) Purposes.—The purposes of this title are—
(1) to increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism;
(2) to ensure that—
(A) banking transactions and financial relationships and the proceeds of criminal transactions and relationships, do not contravene the purposes of subparagraphs of title 3 of title 31, United States Code, section 21 of the Federal Deposit Insurance Act, chapter 2 of title 1 of Public Law 91-508 (84 Stat. 1116), or facilitate the evasion of any such provision; and
(B) the purposes of such provisions of law continue to be fulfilled, and that such provisions of law are effectively and efficiently administered;
(c) to strengthen the provisions put into place by the Money Laundering Control Act of 1986 (18 U.S.C. 981 note), and the International Money Laundering Act of 1994, and to provide a clear national mandate for subjecting to special scrutiny those foreign financial institutions, financial institutions operating outside of the United States, and classes of international transactions that pose particular, identifiable opportunities for criminal abuse;
(d) to ensure that the employment of such measures by the Secretary permits appropriate opportunity for comment by affected financial institutions;
(e) to provide guidance to domestic financial institutions on particular foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions that are of particular, identifiable opportunities for criminal abuse;
(f) to ensure that the forfeiture of any assets in connection with the anti-terrorism efforts of the United States permits for adequate challenge consistent with providing due process rights;
(g) to clarify the terms of the safe harbor from civil liability for filing suspicious activity reports;
(h) to strengthen the authority of the Secretary to issue geographic targeting orders, and to clarify that violations of such orders or any other requirement imposed under the authority contained in chapter 2 of title I of Public Law 91-508 and chapters II and III of title 31, United States Code, may result in criminal and civil penalties;
(i) to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities, and that jurisdictional disputes do not hinder examination of such transactions by financial institutions with relevant reporting requirements;
(j) to fix responsibility for high level coordination of the anti-money laundering efforts of the Department of the Treasury;
(k) to provide additional international anti-money laundering principles and recommendations.

SEC. 221. TRADE SANCTIONS.
(a) In general.—The Trade Sanctions Reform and Export Enhancement Act of 2000 (Public Law 106-387; 114 Stat. 1549A-67) is amended—
(1) by amending section 901(2)(C) to read as follows—
“(C) to facilitate the design, development, or production of chemical or biological weapons, missiles, or weapons of mass destruction;”;
(2) in section 906(a)(1)—
(A) by inserting “, or in the territory of Afghanistan controlled by the Taliban,” after “such country”;
(B) by inserting “, or in the territory of Afghanistan controlled by the Taliban,” after “Korea”;
(C) in section 906(a)(1)—
(D) by inserting “, or in the territory of Afghanistan controlled by the Taliban,” after “such country”;
(E) by inserting “, or in the territory of Afghanistan controlled by the Taliban,” after “Korea”;
(F) in subsection (b) by striking the period at the end of such subsection and inserting in its place a semicolon;
(G) in subsection (C), by striking “the term “country designated pursuant to Executive Order 13224”” and inserting “the term “country designated pursuant to Executive Order 13224, or the territory of Afghanistan controlled by the Taliban””;
(b) Application of the Trade Sanctions Reform and Export Enhancement Act of 2000 shall limit the application or scope of any law establishing criminal or civil penalties, including any executive order or regulation promulgating criminal or civil penalties, including Federal, State, or local laws, or any other requirement for its involvement in international transactions that pose particular, identifiable opportunities for criminal abuse;
(c) nothing in this title shall impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for reasonable expenditures incurred in providing such facilities or technical assistance.

SEC. 222. ASSISTANCE TO LAW ENFORCEMENT AGENCIES.
Nothing in this Act shall impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for reasonable expenditures incurred in providing such facilities or technical assistance.

SEC. 220. NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.
Chapter 121 of title 18, United States Code, is amended—
(1) in section 3730, by striking “under the Federal Rules of Criminal Procedure” every place it appears and inserting “using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation”; and
(2) in section 2711—
(A) in paragraph (1), by striking “and”;
(B) in paragraph (2), by striking the period and inserting “; and”;
(C) by inserting at the end following: “; and
(D) the term “court of competent jurisdiction” has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.”.

SEC. 221. TRADE SANCTIONS.
(a) In general.—The Trade Sanctions Reform and Export Enhancement Act of 2000 (Public Law 106-387; 114 Stat. 1549A-67) is amended—
(1) by amending section 901(2)(C) to read as follows—
“(C) to facilitate the design, development, or production of chemical or biological weapons, missiles, or weapons of mass destruction.”;
(2) in section 906(a)(1)—
(A) by inserting “, the Taliban or the territory of Afghanistan controlled by the Taliban,” after “such country”; and
(B) by inserting “, or in the territory of Afghanistan controlled by the Taliban,” after “Korea”;
(3) in subsection (b) by striking the period at the end of such subsection and inserting in its place a semicolon;
(4) in subsection (C), by striking “the term “country designated pursuant to Executive Order 13224”” and inserting “the term “country designated pursuant to Executive Order 13224, or the territory of Afghanistan controlled by the Taliban””;
(b) Application of the Trade Sanctions Reform and Export Enhancement Act of 2000 shall limit the application or scope of any law establishing criminal or civil penalties, including any executive order or regulation promulgating criminal or civil penalties, including Federal, State, or local laws, or any other requirement for its involvement in international transactions that pose particular, identifiable opportunities for criminal abuse;
(c) nothing in this title shall impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for reasonable expenditures incurred in providing such facilities or technical assistance.
(a) IN GENERAL.—The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(1) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) FORM OF RECORDS AND REPORTS.

(C) SUBMISSION OF REPORTS.

(2) TRANSACTIONS THROUGH ACCOUNTS—

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(3) DEDUCTION OF FEE OR OTHER AMOUNTS.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(4) COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(5) PROHIBITIONS OR CONDITIONS ON OPENING OR MAINTAINING UNAUTHORIZED ACCOUNTS.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(6) DETERMINATION OF PRIMARY MONEY LAUNDERING CONCERN.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(7) DETERMINATION OF PRIMARY MONEY LAUNDERING CONCERN.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(8) DETERMINATION OF PRIMARY MONEY LAUNDERING CONCERN.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(9) DETERMINATION OF PRIMARY MONEY LAUNDERING CONCERN.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.

(10) DETERMINATION OF PRIMARY MONEY LAUNDERING CONCERN.

(A) IN GENERAL. The Secretary may require any financial institution operating outside of the United States, or a correspondent account through which such financial institution conducts, as a condition of opening or maintaining such account, the financial institution operating outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the appropriate banking agency, may determine to be reasonable and practicable to obtain the information:

(B) RECORDKEEPING AND REPORTING OF CASH TRANSACTIONS.

(C) SUBMISSION OF REPORTS.
through account by any domestic financial institution or domestic financial agency for or on behalf of a foreign banking institution, if such correspondent account or payable-through account involves any such jurisdiction or institution, or if any such transaction may be conducted through such correspondent account or payable-through account.

“(c) CONSULTATIONS AND INFORMATION TO BE CONSIDERED IN FINDING JURISDICTIONS, INSTITUTIONS, TYPES OF ACCOUNTS, OR TRANSACTIONS TO BE OF PRIMARY MONEY Laundering CONCERN.—

(1) IN GENERAL.—In making a finding that results in a finding described in paragraph (1), the Secretary shall consider in addition such information as the Secretary determines to be relevant, including the following potentially relevant factors:

(A) JURISDICTIONAL FACTORS.—In the case of a finding described in paragraph (1), the Secretary shall consult with the Secretary of State, the Attorney General, the Secretary of the Treasury, and the Commissioner of Internal Revenue regarding the following:

(i) evidence that criminal groups, international terrorists, or both, have transacted business in that jurisdiction;

(ii) the extent to which that jurisdiction is characterized as a tax haven or offshore banking center and the extent to which that jurisdiction offers bank secrecy or special tax or regulatory advantages to nonresident individuals or nontaxpayers of that jurisdiction;

(iii) the substance and quality of administration of the bank supervisory and counter-money laundering laws of that jurisdiction;

(iv) the relationship between the volume of financial transactions occurring in that jurisdiction and the size of the economy of the jurisdiction;

(v) the extent to which that jurisdiction is characterized as a tax haven or offshore banking center and the extent to which that jurisdiction offers bank secrecy or special tax, or regulatory advantages to nonresident individuals or nontaxpayers of that jurisdiction;

(vi) whether the United States has a mutual bank secrecy treaty with that jurisdiction, and the experience of United States law enforcement officials, regulatory officials, and tax administrators in obtaining information about transactions occurring in or routed through to or from that jurisdiction; and

(vii) the extent to which that jurisdiction is characterized by high levels of official or institutional corruption.

(B) INSTITUTIONAL FACTORS.—In the case of a decision to apply 1 or more of the special measures described in subsection (a)(1), the Secretary shall, after consultation with representatives of the Senate Banking, Housing, and Urban Affairs Committee and the Committee on Finance of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate of any such action.

(g) STUDY AND REPORT ON FOREIGN NA-

(1) STUDY.—The Secretary, in consultation with the appropriate Federal agencies, including the Federal banking agencies (as defined in section 3 of the Federal Deposit Insurance Act), shall conduct a study to:

(A) determine the most effective and efficient means of tracking foreign financial institutions and their ownership, and publish that information as the Secretary determines to be appropriate; and

(B) consider the need for requiring foreign financial institutions to adopt an identification number, similar to what is required for United States citizens through a social security number or tax identification number, prior to opening a correspondent account with a domestic financial institution.

(2) REPORT.—The Secretary shall report to Congress not later than 180 days after the date of enactment with recommendations for implementing such action referred to in paragraph (1) in a timely and effective manner.

(r) DESIGNATIONS.—Notwithstanding any other provision of this chapter, for purposes of this section, the following definitions shall apply:

(1) BANK DEFINITIONS.—The following definitions shall apply with respect to a bank:

(A) ACCOUNT.—The term ‘account’—

(i) means a financial account of a correspondent account in the United States or a financial account that a financial institution other than a bank, the Secretary shall, after consultation with representatives of the Senate Banking, Housing, and Urban Affairs Committee and the Committee on Finance of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate of any such action.

(2) MINIMUM STANDARDS FOR COR-

(1) ACCOUNT.—The term ‘correspondent account’ means an account established to receive deposits from, make payments on behalf of, or otherwise conduct financial transactions related to such institution.

(2) PAYABLE-THROUGH ACCOUNT.—The term ‘payable-through account’ means an account established to receive deposits from, make payments on behalf of, or otherwise conduct financial transactions related to such institution.

SEC. 312. SPECIAL DUE DILIGENCE FOR COR-

(a) IN GENERAL.—Subparagraph (B) shall apply if a correspondent account is requested or maintained by, or on behalf of, a foreign bank operating—

(i) under an offshore banking license; or

(ii) to conduct enhanced scrutiny of such account to guard against money laundering and report any suspicious transactions under section 5318A, as applicable.

(b) POLICIES, PROCEDURES, AND CON-

(i) to ascertain whether such foreign bank provides correspondent accounts to other foreign banks and, if so, the identity of those foreign banks and the information contained in the information as the Secretary determines to be appropriate under paragraph (1).
“(b) is subject to supervision by a banking authority in the country regulating the affiliated depository institution, credit union, or foreign bank described in subparagraph (A), as applicable, that has a physical presence; and

(4) Definitions.—For purposes of this subsection—

(A) the term ‘affiliate’ means a foreign bank that is controlled by or is under common control with a depository institution, credit union, or foreign bank; and

(B) the term ‘physical presence’ means a place of business that—

(i) is maintained by a foreign bank;

(ii) is located at a fixed address (other than solely an electronic address) in a country by which the foreign bank is authorized to conduct banking activities, at which location the foreign bank—

(1) employs 1 or more individuals on a full-time basis; and

(2) maintains operating records related to its banking activities; and

(iii) is subject to inspection by the banking authority which licensed the foreign bank to conduct banking activities.”.

SEC. 314. COOPERATIVE EFFORTS TO DETECT FOREIGN SHELL BANKS.

(a) Cooperation Among Financial Institutions, Regulatory Authorities, and Law Enforcement Authorities.—

(1) Regulations.—The Secretary shall, withing 120 days after the date of enactment of this Act, adopt regulations to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with each other information concerning individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities.

(2) CONTENTS.—The regulations promulgated pursuant to paragraph (1) may—

(A) require that each financial institution designate 1 or more persons to receive information concerning, and to monitor accounts of, individuals, entities, and organizations identified, pursuant to paragraph (1); and

(B) further establish procedures for the protection of the shared information, consistent with the capacity, size, and nature of the institution to which the particular procedures apply.

(3) RULE OF CONSTRUCTION.—The receipt of information by a financial institution pursuant to this section shall not be used for any purpose other than identifying and reporting on activities that may relate to terrorist acts or money laundering activities.

(b) Cooperation Among Financial Institutions.—Upon request, the Secretary, 2 or more financial institutions and any other institution, may share information regarding individuals, entities, and organizations suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, reports, or shares information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall be subject to the remedies that may be available to an owner or account holder under any contract or other written agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure, except where the claim is based on a claim that the disclosure or the failure to provide notice of the disclosure violates this section or regulations promulgated pursuant to this section.

SEC. 315. INCLUSION OF FOREIGN CORRUPTION OFFENSES AS MONEY LAUNDERING CRIMES.

Section 1956(c) of title 18, United States Code, is amended—

(1) in clause (ii), by striking “or destruction of property by means of explosive or fire” and inserting “or destruction of property by means of explosive or fire, or a crime of violence”;

(2) in clause (ii), by striking “1978” and inserting “1978”;

and

(3) by adding at the end the following:—

(iv) bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official;

(v) smuggling or export control violations involving—

(I) an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

(II) an item controlled under regulations under the Export Administration Act of 1977 (15 C.F.R. Parts 730–774);

(vi) an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States; or

(vii) the misuses of funds of, or provided by, the International Monetary Fund in contravention of the Articles of Agreement of the Fund or the misuse of funds of, or provided by, any other international financial institution (as defined in section 1701(c)(2) of the International Financial Institutions Act (22 U.S.C. 262r(c)(2)) in contravention of any treaty or other instrument to which the United States is a party, including any articles of agreement of the members of the international financial institution”;

SEC. 316. ANTI-TERRORIST FORFEITURE PROTECTION.

(a) Right to Contest.—An owner of property that is confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (28 U.S.C. 1738); or

(b) Evidence.—In considering a claim filed under this section, the Government may rely on evidence that is otherwise inadmissible under the Federal Rules of Evidence, if a court determines that such reliance is necessary to protect the national security interests of the United States.
of property under section 593 of title 18, United States Code, or any other provision of law.

SEC. 317. LONG-ARM JURISDICTION OVER FOREIGN FINANCIAL INSTITUTIONS.

Section 1565(b) of title 18, United States Code, is amended—

(1) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively, and moving the margins 2 cms to the right; and

(2) by inserting after ‘‘(b)’’ the following:

‘‘(c) If a bank records request has been received by a covered financial institution, the institution shall provide the information to the requesting officer not later than 120 days after receipt of the request. Upon receipt of a written request from a Federal law enforcement officer for information related to anti-money laundering or terrorist financing, a covered financial institution shall provide the information to the requesting officer not later than 7 days after receipt of the request. Not later than 10 business days after receipt of written notice from the Secretary or the Attorney General that a foreign bank has failed to—

(i) to comply with a summons or subpoena issued under subparagraph (A); or

(ii) to maintain records of a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

‘‘(iii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States and the name and address of a person who resides in the United States and is authorized to accept service of legal process for records relating to the corresponding account. The covered financial institution shall provide the information to the requesting officer not later than 7 days after receipt of the request.

‘‘(iv) TERMINATION OF CORRESPONDENT RELATIONSHIP.—

(ii) if a covered financial institution which maintains a correspondent account in the United States for a foreign bank shall maintain records in the United States identifying the owners of such foreign bank and the covered financial institution shall provide the information to the requesting officer not later than 7 days after receipt of the request.

‘‘(ii) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the covered financial institution shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

‘‘(c) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

‘‘(c) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

‘‘(c) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

‘‘(c) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

‘‘(c) BANK RECORDS RELATED TO ANTI-MONEY LAUNDERING PROGRAMS.—(1) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

(A) APPROPRIATE FEDERAL BANKING AGENCY.—The term ‘appropriate Federal banking agency’ has the same meaning as in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(B) INCORPORATED TERMS.—The terms ‘correspondent account’, ‘covered financial institution’, and ‘foreign bank’ have the same meanings as in section 5318A.

(2) 120-HOUR RULE.—Not later than 120 hours after receiving a request by an appropriate Federal banking agency for information related to anti-money laundering compliance by a covered financial institution or to avoid forfeiture of funds, the appropriate Federal banking agency shall provide the appropriate Federal banking agency, information and account documentation for any account opened, maintained, administered or managed in the United States by the covered financial institution.

‘‘(b) FOREIGN BANK RECORDS.—

(A) SUMMONS OR SUBPOENA OF RECORDS.—

(i) IN GENERAL.—The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.

(ii) SERVICE OF SUMMONS OR SUBPOENA.—A summons or subpoena referred to in clause (i) may be served on the foreign bank in the United States by the covered financial institution which maintains a correspondent account in the United States

S10614 CONGRESSIONAL RECORD — SENATE October 11, 2001
“(II) to initiate proceedings in a United States court contesting such summons or subpoena.

“(ii) LIMITATION ON LIABILITY.—A covered financial institution shall not be liable to any person in any court or arbitration proceeding for terminating a correspondent relationship in accordance with this subsection.

“(iii) FAILURE TO TERMINATE RELATIONSHIP.—Failure to terminate a correspondent relationship in accordance with this subsection shall render the covered financial institution liable for a civil penalty of up to $10,000 per day until the correspondent relationship is so terminated.

“(c) Financial institutions affected by section 5333 of title 31 United States Code, as amended by this title, shall have 60 days from the date of enactment of this Act to comply with the provisions of that section.

(d) Requests for Records.—Section 348A(a)(1) of title 18, United States Code, is amended by striking ‘‘, or (II) a Federal offense involving the sexual exploitation or abuse of children’’ and inserting ‘‘, or (III) a Federal offense involving the sexual exploitation or abuse of children, or (III) money laundering, in violation of section 1956, 1957, or 1960 of title 18’’.

(e) Authority To Order Convicted Criminal To Return Property Located Abroad.—

(1) FORFEITURE OF SUBSTITUTE PROPERTY.—Section 413(p) of the Controlled Substances Act (21 U.S.C. 853) is amended to read as follows:

“(1) FORFEITURE OF SUBSTITUTE PROPERTY.—

“(i) In general.—Paragraph (2) of this subsection shall apply, if any property described in subparagraph (a), as a result of any act or omission of the defendant—

“(A) cannot be located upon the exercise of due diligence; or

“(B) has been transferred or sold to, or deposited with, a third party;

“(C) has been beyond the jurisdiction of the court; or

“(D) has been substantially diminished in value; or

“(E) has been commingled with other property which cannot be divided without difficulty.

“(ii) SUBSTITUTE PROPERTY.—In any case described in any of subparagraphs (A) through (E) of paragraph (1), the court may, at the discretion of the court, order the forfeiture of any other property of the defendant, up to the value of any property described in subparagraphs (A) through (E) of paragraph (1), as applicable.

“(iii) RETURN OF PROPERTY TO JURISDICTION.—In the case of property described in paragraph (1)(C), the court may, in addition to any other action authorized by this subsection, order the defendant to return the property to the jurisdiction of the court so that the property may be seized and forfeited.

(2) PROTECTIVE ORDERS.—Section 413(e) of the Controlled Substances Act (21 U.S.C. 853(e)) is amended by adding at the end the following:

“(4) ORDER TO REPEATE CHARGE AND DEPOSIT.—

“(A) In general.—Pursuant to its authority to enter a pretrial restraining order under this section, including its authority to restrain any property forfeitable as substitute assets, the court may order a defendant to repatriate any property that may be seized, forfeited, and to deposit that property pending trial in the registry of the court, or with the United States Marshals Service or the Secretary of the Treasury, in an interest-bearing account, if appropriate.

“(B) Failure to comply.—Failure to comply with an order under this subsection, or an order to repatriate property under subsection (p), shall be punishable as a civil or criminal contempt of court, and may also result in an enhancement of the sentence of any defendant found to be in violation of just exception provision of the Federal Sentencing Guidelines.”.

SEC. 320. PROCEEDS OF FOREIGN CRIMES.

Section 1956(a)(1)(B) of title 18, United States Code, is amended to read as follows:

“(B) Any property, real or personal, within the jurisdiction of the United States, constituting, derived from, or traceable to, any proceeds obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense—

“(1) involves the manufacture, importation, sale, or distribution of a controlled substance (as that term is defined for purposes of the Controlled Substances Act), or any other conduct described in section 1966(c)(1)(B);

“(ii) would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding 1 year; and

“(iii) would be punishable under the laws of the United States by imprisonment for a term exceeding 1 year, if the act or activity constituting the offense had occurred within the jurisdiction of the United States.”.

SEC. 321. EXEMPTIONS FROM FORFEITURE OF PROCEEDS OF FOREIGN JURISDICTIONS.

Section 2265(c)(2) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(a)(2)) is amended by adding at the end the following:

“(1) MONEY LAUNDERING ACTIVITIES.—Any alien who the consular officer or the Attorney General knows or has reason to believe is in possession of, or has engaged in, activities which, if engaged in within the United States would constitute a violation of section 1956 or 1957 of title 18, United States Code, or has been a knowing conspirator or co-conspirator or co-conspirator with others in any such illicit activity is inadmissible.”.

SEC. 322. CORPORATION REPRESENTED BY A FUGITIVE.

Section 2266 of title 18, United States Code, is amended by designating the present matter as subsection (a), and adding at the end the following:

“(b) Subsection (a) may be applied to all stocks or bonds held by a corporation the claim on behalf of the corporation is a person to whom subsection (a) applies.”.

SEC. 323. CONCENTRATION ACCOUNTS.

Section 2676 of title 28, United States Code, is amended in subsection (d), by adding the following after paragraph (2):

“(3) PRESERVATION OF PROPERTY.—To preserve the availability of property subject to a foreign forfeiture or confiscation judgment, the Government may apply for, and the court may issue, a restraining order pursuant to section 963(j) of title 18, United States Code. The Secretary of the Treasury may file an application is filed pursuant to subsection (c)(1). The court, in issuing the restraining order—

“(A) may rely on information set forth in an affidavit describing the nature of the proceeding investigation underway in the foreign country, and setting forth a reasonable basis to believe that the property to be re-

“strained will be named in a judgment of for- feiture at the conclusion of such proceeding; or

“(B) may register and enforce a restraining order has been issued by a court of competent jurisdiction in the foreign country and certified by the Attorney General pursuant to section 5318A, or any regulation prescribed under section 5318 or any special measures imposed under section 5318A, shall be fined in an amount to not less than 2 times the amount of the transaction, but not more than $1,000,000.”.

SEC. 324. REPORT AND RECOMMENDATION.

Not later than 30 months after the date of enactment of this Act, the Secretary, in consultation with the Attorney General, the System agencies, the Banking agencies (as defined in section 3 of the Federal Deposit Insurance Act), the Securities and Exchange Commission, and such other agencies as the Secretary determines, shall evaluate the operations of the provisions of this subtitle and make recommendations to Congress as to any legislative action with respect to this subtitle as the Secretary may determine to be necessary or advisable.

SEC. 325. REPORT ON EFFECTIVENESS.

The Secretary shall report annually on measures taken pursuant to this subtitle, and shall submit the report to the Committee on Banking, Housing, and Urban Af-

ness, the Senate and the Committee on Financial Services of the House of Repre-

sentatives.

SEC. 327. CONCENTRATION ACCOUNTS AT FINAN-

CIAL INSTITUTIONS.

Section 5318(b) of title 31, United States Code, as amended by section 202 of this title, is amended by adding at the end the following:

“(3) CONCENTRATION ACCOUNTS.—The Sec-

“retary may issue regulations under this sub-

section that govern maintenance of con-

centrated accounts at financial institu-

“tions, in order to ensure that such accounts are not used to prevent association of the
identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner, which regulations shall, at a minimum—

"(1) prohibit financial institutions from allowing clients to direct transactions that move their funds into, out of, or through the concentration accounts of the financial institution; and

"(2) require each financial institution to establish and maintain procedures governing the documentation of all transactions involving a concentration account, which procedures shall ensure that, any time a transaction involving a concentration account commingles funds belonging to 1 or more customers, the identity of, and specific amount belonging to, each customer is documented.

Subtitle B—Currency Transaction Reporting

Amendments and Related Improvements

SEC. 331. AMENDMENTS RELATING TO REPORTING OF SUSPICIOUS ACTIVITIES.

(a) AMENDMENT RELATING TO CIVIL LIABILITY RELATING TO CIVIL LIABILITY—Amendment to section 5318(g)(3) of title 31, United States Code, is amended to read as follows:

'(g) AMENDMENT RELATING TO CIVIL LIABILITY—(3) a financial institution shall, at a minimum—

'(A) disclose to any person who is the subject of such disclosure or any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

'(B) RULE OF CONSTRUCTION.—Subparagraph (A) shall not be construed as creating—

'"(i) any inference that the term 'person', as used in such subparagraph, may be construed more broadly than its ordinary usage so as to include any government or agency of government; or

'"(ii) any immunity against, or otherwise affecting, any civil or criminal action brought by any government or agency of government to enforce any constitution, law, or regulation of such government or agency; or

'(c) require each financial institution to establish and maintain procedures governing the documentation of all transactions involving a concentration account, which procedures shall ensure that, any time a transaction involving a concentration account commingles funds belonging to 1 or more customers, the identity of, and specific amount belonging to, each customer is documented.'

(b) PROHIBITION ON NOTIFICATION OF DISCLOSURES.—Section 5318(g)(2) of title 31, United States Code, is amended to read as follows:

'(2) NOTIFICATION PROHIBITED.—(A) a financial institution or any director, officer, employee, or agent of any financial institution, voluntarily or pursuant to this section or any other authority, reports a suspicious transaction to a government agency—

'"(i) the financial institution, director, officer, employee, or agent may not notify any person involved in the transaction that the transaction has been reported; and

'"(ii) no officer or employee of the Federal Government or of any State, local, tribal, or territorial government within the United States, who has any knowledge that such report was made may disclose to any person involved in the transaction that the transaction has been reported.

'(B) DISCLOSURES.—'(i) RULE OF CONSTRUCTION.—Notwithstanding the application of subparagraph (A) in any report under paragraph (A) shall not be construed as prohibiting any financial institution, or any director, officer, employee, or agent of such institution, from including information that was included in a report to which subparagraph (A) applies—

'"(i) in a written employment reference that is provided in accordance with section 5318(g)(3) of this title, in response to a request from another financial institution, except that such written reference may not disclose that such information was also included in such report or that such report was made; or

'"(ii) in a written termination notice or employment reference that is provided in accordance with the rules of the self-regulatory organizations registered with the Securities and Exchange Commission, except that such written notice or reference may not disclose that such information was also included in any such report or that such report was made.

'(ii) INFORMATION NOT REQUIRED.—Clause (1) shall not be construed, by itself, to create any affirmative duty to include any information described in clause (1) in any employment reference or termination notice referred to in clause (1).

SEC. 332. ANTI-MONEY LAUNDERING PROGRAMS.

Section 331(h) of title 31, United States Code, is amended to read as follows:

'(h) ANTI-MONEY LAUNDERING PROGRAMS.—

'(1) IN GENERAL.—In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs, including, at a minimum—

'"(A) the development of internal policies, procedures, and controls;

'"(B) the designation of a compliance officer;

'"(C) an ongoing employee training program; and

'"(D) an independent audit function to test programs.

'(2) REGULATIONS.—The Secretary may prescribe minimum standards for programs established under paragraph (1), and may exempt from the application of those standards any financial institution that is not subject to the provisions contained in part 103 of title 31, of the Code of Federal Regulations, or any successor rule thereto, for so long as such financial institution is not subject to such rules.

SEC. 333. PENALTIES FOR VIOLATIONS OF GEOGRAPHIC TARGETING ORDERS AND CERTAIN RECORDKEEPING REQUIREMENTS, AND LENGTHENING EFFECTIVE PERIOD OF GEOGRAPHIC TARGETING ORDERS.

(a) CIVIL PENALTY FOR VIOLATION OF TARGETING ORDER.—Section 5321(a)(1) of title 31, United States Code, is amended—

'(1) by inserting a comma after ’’or order issued’’ after ’’subchapter or a regulation prescribed’’; and

'(2) in subsection (b)—

'(A) by inserting ’’or order issued’’ after ’’willfully violating a regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under section 5323(b)’’; and

'(B) by inserting ’’or willfully violating a regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under section 5315 or 5324’’.

(b) CRIMINAL PENALTIES FOR VIOLATION OF TARGETING ORDER.—Section 5321(b) of title 31, United States Code, is amended—

'(1) in subsection (a)—

'(A) by inserting ’’or order issued’’ after ’’willfully violating a regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under section 5323(b)’’; and

'(B) by inserting ’’or willfully violating a regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under section 5315 or 5324’’.

(c) STRUCTURING TRANSACTIONS TO evade TARGETING ORDER OR CERTAIN RECORDKEEPING REQUIREMENTS.—Section 5324(a) of title 31, United States Code, is amended—

'(1) by inserting a comma after ’’shall’’;

'(2) by striking ’’section’’ and inserting ’’section’’;

'(3) in paragraph (1), by inserting ’’, to file a report or to maintain a record required by an order issued under section 5323, or to maintain a record required pursuant to any regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under regulation prescribed under any such section’’; and

'(4) in paragraph (2), by inserting ’’, to file a report or to maintain a record required by an order issued under section 5323, or to maintain a record required pursuant to any regulation prescribed under section 5323, or to maintain a record required pursuant to any regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508, after ’’under regulation prescribed under any such section’’.

(d) LENGTHENING EFFECTIVE PERIOD OF GEOGRAPHIC TARGETING ORDERS.—Section 5324(d) of title 31, United States Code, is amended, by inserting ’’, for more than 60’’ and inserting ’’more than 180’’.

SEC. 334. ANTI-MONEY LAUNDERING STRATEGY.

(a) STRATEGY.—Section 5341(b) of title 31, United States Code, is amended by adding at the end the following:

'(12) DATA REGARDING FUNDING OF TERRORISM.—Data concerning money laundering efforts related to the funding of acts of international terrorism, and efforts directed at the prevention, detection, and prosecution of such funding.

SEC. 335. AUTHORIZATION TO INCLUDE SUSPICIONS OF ILLEGAL ACTIVITY IN WRITTEN EMPLOYMENT REFERENCES.

Section 18 of the Federal Deposit Insurance Act (12 U.S.C. 1829) is amended by adding at the end the following:

'(c) WRITTEN EMPLOYMENT REFERENCES MAY CONTAIN SUSPICIONS OF ININVOLVEMENT IN ILLEGAL ACTIVITY.—'(1) AUTHORITY TO DISCLOSE INFORMATION.—Notwithstanding any other provision of law, any insured depository institution, and any director, officer, employee, or agent of such institution, may disclose an employment reference relating to a current or former institution-affiliated party of such institution which is provided to another insufed institution in response to a request from such other institution, information concerning the possible involvement of such institution-affiliated party in potential or unlawful activity.

'(2) INFORMATION NOT REQUIRED.—Nothing in paragraph (1) shall be construed, by itself, to create any affirmative duty to include any reference described in subparagraph (1) in any employment reference referred to in paragraph (1).

'(3) MALICIOUS INTENT.—Notwithstanding any other provision of law, any insured depository institution may disclose a written employment reference of a current or former institution-affiliated party of such institution which is provided to another insured depository institution, and any director, officer, employee, or agent of such institution, may disclose an employment reference relating to a current or former institution-affiliated party of such institution which is provided to another insured depository institution in response to a request from such other institution, information concerning the possible involvement of such institution-affiliated party in potential or unlawful activity.

'(4) LIABILITY FOR VIOLATION OF WRITTEN EMPLOYMENT REFERENCES.—Any insured depository institution and any director, officer, employee, or agent of such institution may be liable for any willful, wanton, or malicious violation of this subsection, and any such liability shall be in addition to any other remedies provided by law, and may include an award of such other remedies that are equitable or just.
employee, or agent of such institution under this subsection concerning potentially unlawful activity that is made with malicious intent, shall not be shielded from liability from any suit filed in the district courts of:

"(4) DEFINITION.—For purposes of this subsection, the term ‘insured depository institution’ includes any uninsured branch or agency of a foreign bank.

SEC. 336. BANK SECRECY ACT ADVISORY GROUP.


(a) in subsection (a)(1), in the word ‘or’ that follows the word ‘any’, by inserting ‘and’ after the word ‘any’; and

(b) in subsection (a)(2), by inserting ‘or’ after the word ‘any’.

(a) AMENDMENT RELATING TO THE PURPOSES OF THE BANK SECRECY ACT.—Section 5311 of title 31, United States Code, is amended by inserting ‘or critical national infrastructure’ after ‘financial institutions other than those managed by the Internal Revenue Service’.

(b) AMENDMENT RELATING TO REPORTING OF SUSPICIOUS ACTIVITIES.—Section 5318 of title 31, United States Code, is amended by—

(A) in subsection (a), in the second paragraph, by striking ‘by a foreign bank’ and inserting ‘by a foreign bank or a foreign bank subsidiary’; and

(B) in subsection (b), by striking ‘a foreign bank’ and inserting ‘a foreign bank or a foreign bank subsidiary’.

(c) AMENDMENT RELATING TO AVAILABILITY OF REPORTS.—Section 5319 of title 31, United States Code, is amended by—

(A) in subsection (a), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’.

(b) in subsection (b), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’.

(c) in subsection (c), by striking ‘by a person’ and inserting ‘or by a person’.

(d) in subsection (d), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’.

(e) in subsection (e), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’.

SEC. 338. REPORTING OF SUSPICIOUS ACTIVITIES BY SECURITIES BROKERS AND DEALERS; INVESTMENT COMPANY STUDY.

SEC. 340. BANK SECRECY PROVISIONS AND ANTI- TERRORIST ACTIVITIES OF UNITED STATES INTELLIGENCE AGENCIES.

(a) AMENDING THE PURPOSES OF THE BANK SECRECY ACT.—Section 5311 of title 31, United States Code, is amended by—

(A) in subsection (a)—

(1) in paragraph (2), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(2) in paragraph (3), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(3) in paragraph (4), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(4) in paragraph (5), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(b) AMENDMENT RELATING TO REPORTING OF SUSPICIOUS ACTIVITIES.—Section 5318 of title 31, United States Code, is amended by—

(A) in subsection (a), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(B) in subsection (b), by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’;

(c) AMENDMENT RELATING TO AVAILABILITY OF REPORTS.—Section 5319 of title 31, United States Code, is amended by—

(A) in subsection (a), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’;

(B) in subsection (b), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’;

(C) in subsection (c), by striking ‘by a person’ and inserting ‘or by a person’;

(D) in subsection (d), by striking ‘includes a foreign bank or a foreign bank subsidiary’ and inserting ‘includes a foreign bank or a foreign bank subsidiary’.

SEC. 337. AGENCY REPORTS ON RECONCILING PENALTY AMOUNTS.

SEC. 339. SPECIAL REPORT ON ADMINISTRATION OF BANK SECRECY ACT PROVISIONS.

SEC. 341. BUDGETARY AND OTHER CONSIDERATION. The report described in section (a) shall specifically address, and contain recommendations concerning—

(A) the adequacy of the mechanisms for the collection of penalties,

(B) the methods by which the reports under section 5314 shall be transmitted,

(C) the compliance of money services businesses and financial institutions with the Bank Secrecy Act.

SEC. 342. BUDGETARY AND OTHER CONSIDERATION.

SEC. 343. BUDGETARY AND OTHER CONSIDERATION.

The Right to Financial Privacy Act of 1978 is amended—

(a) REGULATIONS.—In its report, the Securities and Exchange Commission shall address the following:

(b) AMENDMENT RELATING TO THE PURPOSES OF THE BANK SECRECY ACT.—Section 5311 of title 31, United States Code, is amended by striking ‘foreign bank’ and inserting ‘foreign bank or a foreign bank subsidiary’.

SEC. 344. BUDGETARY AND OTHER CONSIDERATION.

SEC. 345. BUDGETARY AND OTHER CONSIDERATION.
“(c) A Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.”.

(g) AMENDMENT TO THE FAIR CREDIT REPORTING ACT.—The Fair Credit Reporting Act (5 U.S.C. 1681 et seq.) is amended by adding at the end the following new section:

SEC. 342. USE OF AUTHORITY OF UNITED STATES EXECUTIVE DIRECTORS.

(a) ACTION BY THE PRESIDENT.—If the President determines that a particular foreign country has taken or has committed to take measures that support any loan or other utilization of the United States to respond to, deter, or prevent acts of international terrorism, the Secretary of the Treasury may, in accordance with the provisions of this section, take such actions as the President determines are necessary to support any loan or other utilization of the United States to respond to, deter, or prevent acts of international terrorism for the purpose of international financial institution to use the funds to support any loan or other utilization of the United States to respond to, deter, or prevent acts of international terrorism.

(b) USE OF VOICE AND VOTE.—The Secretary of the Treasury shall consult with the Secretary of State and the Director of the Central Intelligence Agency before taking any action under subsection (a).

(c) DEFINITION.—For purposes of this section, the term “international financial institution” means an international financial institution described in section 1701(c)(2) of the International Financial Institutions Act (22 U.S.C. 262c(c)(2)).

Subtitle C—Currency Crimes

SEC. 351. BULK CASH SMUGGLING.

(a) FINANCIAL CRIME.—(1) In general.—The president determines that—

(1) effective enforcement of the currency reporting requirements of chapter 53 of title 31, United States Code (commonly referred to as the Bank Secrecy Act) is insufficient to require changes in the behavior of international financial institutions.

(2) international financial institutions regularly report information to the United States on transactions that are not reported to the United States by their domestic counterparts.

(3) the transportation and smuggling of currency into or out of the United States and from place to place within the United States.

(4) the purpose of bulk cash smuggling is to evade currency reporting requirements.

(b) PENALTIES.

(1) IN GENERAL.—In general, any person who engages in bulk cash smuggling is guilty of a crime punishable by imprisonment for not more than 10 years, or a fine of not more than $250,000, or both.

(2) FORFEITURE.—In addition to any other penalty prescribed by law, any person engaged in bulk cash smuggling is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(c) SEIZURE OF SMUGGLING CASH.

(1) IN GENERAL.—Any property involved in a violation of section 531 of title 31, United States Code, is subject to seizure under section 413 of the Controlled Substances Act (21 U.S.C. 853). If the property subject to forfeiture is not subject to seizure under section 413 of the Controlled Substances Act, the court shall order that the defendant forfeit to the United States any property, real or personal, involved in the offense, and any property traceable to such property, subject to subsection (d).

(2) APPlicABILITY OF OTHER LAWS.—The seizure, restraint, and forfeiture of property under this section shall be governed by section 419 of the Controlled Substances Act (21 U.S.C. 855). If the property subject to forfeiture is unavailable, and the defendant has no substitute property that may be forfeited pursuant to section 419 of the Controlled Substances Act, the court shall enter a personal money judgment against the defendant in an amount equal to the value of the unavailable property.

SEC. 353. BULK CASH SMUGGLING.

(a) FINANCIAL CRIME.—(1) In general.—Any person who engages in, or conspires to engage in, bulk cash smuggling offenses, shall be imprisoned for not more than 10 years, or a fine of not more than $250,000, or both. In determining the sentence, the court shall impose a term of imprisonment of not more than 5 years, or a fine of not more than $500,000, or both.

(2) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(3) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(4) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(5) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(6) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.

(7) Forfeiture.—In addition to any other penalty prescribed by law, any person engaged in, or conspired to engage in, bulk cash smuggling offenses is subject to the forfeiture of any property, real or personal, used to facilitate the crime.
to commit such violation, and any property traceable thereto, may be seized and, subject to subsection (d), forfeited to the United States.

(2) APPLICABLE PROCEDURES.—A seizure and forfeiture under this subsection shall be governed by the procedures governing civil forfeitures under section 581(a)(1)(A) of title 18, United States Code, except—

(d) PROPORTIONALITY OF FORFEITURE.—

(1) MITIGATION.—Upon a showing by the property owner by a preponderance of the evidence that the property or monetary instrument involved in the offense gave rise to the forfeiture, the court shall order the defendant to forfeit all property, real or personal, involved in the offense and any property traceable thereto.

(2) PROVISIONAL ORDER.—Upon a showing by the property owner by a preponderance of the evidence that the property or monetary instrument involved in the offense gave rise to the forfeiture, the court shall order the defendant to forfeit all property, real or personal, involved in the offense and any property traceable thereto.

(3) MITIGATION.—In a forfeiture case under this subsection, upon a showing by the property owner by a preponderance of the evidence that the property or monetary instrument involved in the offense gave rise to the forfeiture, the court shall reduce the forfeiture to the maximum amount that is not grossly disproportional to the gravity of the offense. In determining the amount of the forfeiture, the court may take into account aggravating and mitigating facts and circumstances that have a bearing on the gravity of the offense. Such circumstances include, but are not limited to, the following: the value of the currency or other monetary instrument involved in the offense; efforts by the person committing the offense to conceal or transport the currency or other monetary instrument used or intended to be used to conceal the offense, and any property traceable to the offense; the amount of the forfeiture under subsection (a) or a conspiracy to commit such violation, and any property traceable to the offense; and any property used or intended to be used to facilitate the offense.

(e) RULE OF CONSTRUCTION.—For purposes of subsections (b) and (c), any currency or other monetary instrument that is concealed or intended to be concealed in violation of subsection (a) or a conspiracy to commit such violation, any article, container, or conveyance used or intended to be used to conceal or transport the currency or other monetary instrument, and any other property used or intended to be used to facilitate the offense, shall be considered property involved in the offense.

(2) CRIEAL AMENDMENT.—The table of sections for chapter 53 of title 31, United States Code, is amended by inserting after the item relating to section 5330 the following new item:

5331. Bulk cash smuggling.

(d) CIVIL FORFEITURE VIOLATIONS.—Section 5317(c) of title 31, United States Code, is amended to read as follows:

(1) FORFEITURE OF PROPERTY.—

(1) IN GENERAL.—(A) CRIMINAL FORFEITURE.—The court, in imposing sentence for any violation of section 5131, 5132, or 5324, or any conspiracy to commit such violation, shall order the defendant to forfeit all property, real or personal, involved in the offense and any property traceable thereto.

(2) CIVIL FORFEITURE.—Any property involved in a violation of section 5131, 5132, or 5324, or any conspiracy to commit such violation, and any property traceable thereto, may be seized and, subject to paragraph (3), forfeited to the United States in accordance with the procedures governing civil forfeitures in money laundering cases pursuant to section 581(a)(1)(A) of title 18, United States Code.

(3) MITIGATION.—In a forfeiture case under this subsection, upon a showing by the property owner by a preponderance of the evidence that the property or monetary instrument involved in the offense gave rise to the forfeiture, the court shall reduce the forfeiture to the maximum amount that is not grossly disproportional to the gravity of the offense. In determining the amount of the forfeiture, the court may take into account aggravating and mitigating facts and circumstances that have a bearing on the gravity of the offense. Such circumstances include, but are not limited to, the following: the value of the currency or other monetary instrument involved in the offense; efforts by the person committing the offense to structure currency transactions, conceal property, or otherwise obstruct justice; and whether the offense is part of a pattern of repeated violations.

(e) CONFORMING AMENDMENTS.—Title 18, United States Code, is amended—

(1) in section 981(a)(1)(A) by striking “of section 5313(a) or 5324(a) of title 31”, and

(2) in section 981(a)(1), striking “of section 5313(a), 5316, or 5324 of title 31”,

Subtitle E—Anticorruption Measures

SEC. 361. CORRUPTION OF FOREIGN GOVERNMENTS AND RULING ELITES.

It is the sense of Congress that—

(1) the United States should take the necessary countermeasures to protect the United States against and prevent the transmittal of funds to and from terrorists and terrorist organizations;

(2) the United States should encourage such other country to take action which would identify and prevent the transmittal of funds to and from terrorists and terrorist organizations; and

(3) the United States should encourage such other country to take action which would identify and prevent the transmittal of funds to and from terrorists and terrorist organizations.

TITLE IV—PROTECTING THE BORDER

Subtitle A—Protecting the Northern Border

SEC. 401. ENSURING ADEQUATE PERSONNEL ON THE NORTHERN BORDER.

The Attorney General is authorized to waive any FTE cap on personnel assigned to the Immigration and Naturalization Service to address the national security needs of the United States on the Northern border.

SEC. 402. NORTHERN BORDER PERSONNEL.

There are authorized to be appropriated—

(1) such sums as may be necessary to triple the number of Border Patrol personnel (from the number authorized under current law), and the necessary personnel and facilities to support such personnel, in each State along the Northern Border;

(2) such sums as may be necessary to triple the number of Customs Service personnel (from the number authorized under current law), and the necessary personnel and facilities to support such personnel, at ports of entry in each State along the Northern Border;

(3) such sums as may be necessary to triple the number of INS inspectors (from the number authorized on the date of enactment of this chapter), and the necessary personnel and facilities to support such personnel, at ports of entry in each State along the Northern Border; and

(4) an additional $50,000,000 each to the Immigration and Naturalization Service and the United States Customs Service for purposes of making improvements in technology for monitoring the Northern Border and acquiring additional equipment at the Northern Border.

SEC. 403. ACCESS BY THE DEPARTMENT OF STATE AND THE INS TO CERTAIN IDENTIFYING INFORMATION IN THE CRIMINAL HISTORY RECORDS OF VISA APPLICANTS AND APPLICANTS FOR ADMISSION TO THE UNITED STATES.

(a) AMENDMENT OF THE IMMIGRATION AND NATIONALITY ACT.—Section 105 of the Immigration and Nationality Act (8 U.S.C. 1105) is amended—

(1) in the section heading, by inserting “; DATA EXCHANGE” after “SECURITY OFFICERS”;

(2) by inserting “(a)” after “SEC. 105,”

(3) in subsection (a), by inserting “and border” after “internal” the second place it appears; and

(4) by adding at the end the following:

“(1) The Attorney General and the Director of the Federal Bureau of Investigation shall provide the Department of State and the Service access to the criminal history information contained in the National Crime Information Center’s Interstate Identification Index (NCIC-III), Wanted Persons File, and other such files maintained by the National Crime Information Center that may be mutually agreed upon by the Attorney General and the agency receiving the access, for the purpose of determining whether or not a visa applicant or applicant for admission has a criminal history record indexed in any such file.

“Such access shall be provided by means of extracts of the records for placement in the automated visa lookup or other
appropriate database, and shall be provided without any fee or charge.

(3) The Federal Bureau of Investigation shall provide periodic updates of the extracts at intervals mutually agreed upon with the agency receiving the access. Upon receipt of such updated extracts, the receiving agency shall make corresponding updates to its database and destroy previously provided extracts.

(4) Access to an extract does not entitle the Department of State to obtain the full content of the corresponding automated criminal history record. To obtain the full content of the criminal history record, the Department of State shall submit the applicant's fingerprints and any appropriate fingerprint processing fee authorized by law to the National Identification Information Services Division of the Federal Bureau of Investigation.

(c) The provision of the extracts described in subsection (b) may be reconsidered by the Attorney General and the receiving agency upon the development and deployment of a more efficient means of sharing the information.

(d) For purposes of administering this section, the Department of State shall, prior to receiving access to NCIC data not later than 4 months after the date of enactment of this subsection, promulgate final regulations.

(1) to implement procedures for the taking of fingerprints; and

(2) to establish the conditions for the use of the fingerprints. The Attorney General or the Secretary of State, as determined by regulation, shall submit the appropriate database, and shall be provided with the fingerprints and any appropriate fingerprint processing fee authorized by law to the National Identification Information Services Division of the Federal Bureau of Investigation.

The provision of the extracts described in subsection (b) may be reconsidered by the Attorney General and the receiving agency upon the development and deployment of a more efficient means of sharing the information.

(2) To ensure that such information is used solely to determine whether or not to issue a visa to an alien or to admit an alien to the United States.

(3) To ensure the security, confidentiality, and destruction of such information; and

(4) To protect any privacy rights of individuals who are subjects of such information.

(b) Reporting Requirement.—Not later than 2 years after the date of enactment of this Act, the Attorney General and the Secretary of State jointly shall report to Congress on the implementation of the amendments made by this section.

(c) Technology Standard to Confirm Identity.—

(1) In General.—The Attorney General and the Secretary of State jointly, through the National Institute of Standards and Technology (NIST), and in consultation with the Secretary of the Treasury and other Federal agencies or officers authorized to enforce the Immigration and Nationality Act, shall develop a technology standard and electronic database system described in this subsection.

(2) Integrated.—The technology standard developed pursuant to paragraph (1), shall be the technological basis for a cross-agency, cross-platform electronic system that is a cost-effective, efficient, fully integrated means to share law enforcement and intelligence information necessary to confirm the identity of such persons applying for a United States visa or such person seeking to enter the United States pursuant to a visa.

(a) In General.—In consultation with the appropriate heads of other Federal agencies or officers authorized to enforce the Immigration and Nationality Act, the Secretary of State, Secretary of the Treasury, and the Secretary of Transportation, shall report to Congress on the feasibility of integrating the Integrated Automated Fingerprint Identification System (IAFIS) of the Federal Bureau of Investigation and other identification systems in order to better identify a person who holds a foreign passport or visa and may be wanted in connection with a criminal investigation in the United States or abroad, before the issuance of a visa to the person entering or exiting the United States.

(b) Authorization of Appropriations.—There is authorized to be appropriated not less than $2,000,000 for fiscal year 2001 and each subsequent fiscal year, to support the implementation of this section.

Subtitle B—Enhanced Immigration Provisions

SEC. 404. LIMITED AUTHORITY TO PAY OVER-TIME.

The matter under the heading “Immigration and Naturalization Service: Salaries and Expenses, Enforcement And Border Affairs” and “Immigration And Naturalization Service: Salaries and Expenses, Citizenship And Benefits, Fiscal Year 2001,” in the Department of Justice Appropriations Act, 2001 (as enacted into law by Appendix B (H.R. 5548) of Public Law 106-553 (114 Stat. 2762A-58 to 2762A-99)), is amended by striking the following each place it occurs:

"Provided, That none of the funds available to the Immigration and Naturalization Service shall be available to pay any employee overtime pay in an amount in excess of $30,000 during the calendar year beginning January 1, 2001."

SEC. 405. REPORT ON THE INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM FOR POINTS OF ENTRANCE AND OVERSEAS CONSULAR POSTS.

(a) In General.—The Attorney General, in consultation with the appropriate heads of other Federal agencies or officers authorized to enforce the Immigration and Naturality Act, shall submit a report to the Comptroller General of the United States on the implementation of the Integrated Automated Fingerprint Identification System (IAFIS) of the Federal Bureau of Investigation and other identification systems in order to better identify a person who holds a foreign passport or visa and may be wanted in connection with a criminal investigation in the United States or abroad, before the issuance of a visa to the person entering or exiting the United States.

(b) Authorization of Appropriations.—There is authorized to be appropriated not less than $2,000,000 for fiscal year 2001 and each subsequent fiscal year, to support the implementation of this section.

IV. Engage in Terrorist Activity Defined.

As used in this chapter, the term "engage in terrorist activity" means, in an individual capacity or as a member of an organization, in each of the following:

"(i) to commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity;"

"(ii) to prepare or plan a terrorist activity;"

"(iii) to gather information on potential targets for terrorist activity;"

"(iv) to solicit funds or other things of value for—"

"(aa) a terrorist activity;"

"(bb) a terrorist organization described in clauses (vi)(I) or (vi)(II); or"

"(cc) a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate that he did not know, and should not reasonably have known, that the solicitation would further the organization's terrorist activity;"

"(V) to solicit any individual to engage in conduct otherwise described in this clause;"

"(bb) a terrorist organization described in clauses (vi)(I) or (vi)(II); or"

"(cc) a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate that he did not know, and should not reasonably have known, that the solicitation would further the organization's terrorist activity;"

"(V) to solicit any individual to engage in conduct otherwise described in this clause;"
“(VI) to commit an act that the
actor knows, or reasonably should know, affords
material support, the including a safe house,
transportation, communications, funds, trans-
fer of funds or other material financial
benefit, false documentation or identifica-
tion, weapons (including chemical, biologi-
cal, or radiological weapons), explosives, or
training;’’

“(aa) for the commission of a terrorist ac-
tivity;”

“(bb) to any individual who the actor
knows, or reasonably should know, has com-
mits or plans to commit a terrorist activity;

“(cc) to a terrorist organization described in
clauses (vi)(I) or (vi)(II); or

“(dd) to a terrorist organization described in
clause (vi)(III), unless the actor can
demonstrate that he did not know, and should
not reasonably have known, that the act
would further the organization’s terrorist ac-
tivity.

“This clause shall not apply to any material
support the alien afforded to an organization
or individual that has committed terrorist
activity, if the Secretary of State, after con-
sultation with the Attorney General, or the
Attorney General, after consultation with the
Secretary of State, concludes in his sole
unreviewable discretion, that this clause
should not apply.

(D) by adding at the end the following new clause:

“(v) TERRORIST ORGANIZATION DEFINED.—As
used in clause (iv)(I) and clause (iv), the
term ‘terrorist organization’ means an or-

“(II) designated under section 219;

“(III) otherwise designated, upon publica-
tion in the Federal Register, by the Sec-

ary of State in consultation with or upon the
request of the Attorney General, or the
Attorney General, after consultation with
the Secretary of State, as a ter-

rorist organization, after finding that it en-
egages in the activities described in clause
(I), (II), or (III) of clause (iv), or that it pro-

vides material support to further terrorist
activity; or

“(III) that is a group of two or more indi-

viduals, whether organized or not, which en-
gages in the activities described in clause
(I), (II), or (III) of clause (iv);”:

and

(2) by adding at the end the following new
paragraph:

“(P) APPLICABILITY WITH TERRORIST ORGAN-
IZATIONS.—Any alien who the Secretary of
State, after consultation with the Attorney
General, or the Attorney General, after con-
sultation with the Attorney General, or the
Secretary of State, has been associated with a ter-

rorist organization and intends while in the
United States to engage solely, principally, or
cidentally in activities that could endanger
the welfare, safety, or security of the United
States is inadmissible.”;

(b) CONFORMING AMENDMENT.—Section
237(a)(10) of the Immigration and Na-

tionality Act (8 U.S.C. 1227(a)(10)) is amended
by striking “section 212(a)(3)(B)(i)(ii)” and
inserting “section 212(a)(3)(B)(i)(iv)”;

(c) RETROACTIVE APPLICATION OF AMEND-
MENTS.—

(1) IN GENERAL.—Except as otherwise pro-

vided in this subsection, the amendments
made by this section shall take effect on the
date of enactment of this Act and shall apply
to—

(A) actions taken by an alien before, on, or
after such date; and

(B) all aliens, without regard to the date of
entry or attempted entry into the United
States;

and

(2) in removal proceedings on or after such
date (except for proceedings in which there has
been a final administrative decision before
the date of enactment of this Act),

(ii) seeking admission to the United States
on or after such date.

(2) SPECIAL RULE FOR ALIENS IN EXCLUSION
OR DEPORTATION PROCEEDINGS.—Notwith-
standing any other provision of law, the
amendments made by this section shall not
apply in a removal or deportation pro-

ceeding on or after the date of en-
actment of this Act (except for proceedings
in which there has been a final administra-
tive decision before such pro-
ceedings were removal proceedings.

(3) SPECIAL RULE FOR SECTION 219 ORGANIZA-
TIONS AND ORGANIZATIONS DESIGNATED UNDER
SECTION 212A.

(A) IN GENERAL.—Notwithstanding para-
graphs (1) and (2), no alien shall be consid-

ered inadmissible under section 212(a)(3) of
the Immigration and Nationality Act (8 U.S.C.
1182(a)(3)), or deportable under section
237(a)(4)(B) of such Act (8 U.S.C.
1227(a)(4)(B)), by reason of the amendments
made by subsection (a), on the ground that the
alien engaged in a terrorist activity de-
scribed in subclause (IV)(bb), (V)(bb),
or (VI)(cc) of section 212(a)(3)(B)(i)(iv) of such
Act (as so amended) with respect to a group at
any time when the group was not a terrorist
organization designated by the Secretary of
State under section 219 of such Act (8 U.S.C.
1189(a)) or otherwise designated under

(B) STATUTORY CONSTRUCTION.—Subpara-
graph (A) shall not be construed to prevent an
alien from being considered inadmissible or
deportable for having engaged in a ter-
rorist activity—

(1) described in subclause (IV)(bb), (V)(bb),
or (VI)(cc) of section 212(a)(3)(B)(iv) of such
Act (as so amended) with respect to a ter-
rorist organization at any time when such
organization was designated by the Sec-

etary of State under section 219 of such Act
(as so amended) with respect to a ter-

rorist organization or deportable for having
engaged in a terrorist activity.

(2) by striking “section 212(a)(3)(B)(i)(ii)” and
inserting “section 212(a)(3)(B)(i)(iv)”;

(3) by describing in subclause (IV)(cc), (V)(cc),
or (VI)(dd) of section 212(a)(3)(B)(iv) of such
Act (as so amended) with respect to a ter-
rorist organization described in section

(4) EXCLUSION.—The Secretary of State, in
consultation with the Attorney General, may
determine that the amendments made by
this section shall not apply with respect to an
alien taken outside the United States before the
date of enactment of this Act upon the recom-

mendation of a designated representative that
there is not reasonable ground to believe
that the alien knew or reasonably should
have known that the actions would further a
terrorist activity.

(c) DESIGNATION OF FOREIGN TERRORIST OR-
GANIZATIONS.—Section 219(a) of the Immi-

gration and Nationality Act (8 U.S.C. 1189(a)) is
amended—

(1) in paragraph (1)(B), by inserting “or
terrorism (as defined in section 101(a)(32) of
the Foreign Relations Authorization Act, Fiscal
Years 1988 and 1989 (22 U.S.C.
2656c(a)(32)))”;

(2) in paragraph (1)(C), by inserting “or ter-
rorist” after “terrorist activity”;

(3) by amending paragraph (2)(A) to read as
follows:

“(A) NOTICE.—

(1) TO CONGRESSIONAL LEADERS.—Seven
days before making a designation under this
subsection, the Secretary shall, by classified

memorandum, notify the Speaker and Mi-

nority Leader of the House of Repre-

sentatives, the President pro tempore, Major-

ity Leader, and Minority Leader of the Senate,
and the members of the relevant commit-
	ee. In making a designation of a terrorist
organization under this subsection, together
with the findings made under paragraph (1)
with respect to that organization, and the
factual basis therefor.

“(ii) PUBLICATION IN FEDERAL REGISTER.—
The Secretary shall publish the designation
in the Federal Register seven days after pro-

viding the notification under clause (1);”;

(4) in paragraph (2)(B)(i), by striking “sub-
paragraph (A)” and inserting “subpara-
graph (A)(ii)”;

(5) in paragraph (2)(C), by striking “para-

graph (2)” and inserting “paragraph (2)(A)(ii)”;

(6) in paragraph (3)(B), by striking “sub-
section (c)” and inserting “subsection (b)”;

(7) in paragraph (4)(B), by inserting after
the second sentence the following: “The Sec-

retary also may redesignate such organiza-

tion at the end of any 2-year redesignation
period (but not sooner than 60 days prior to
the expiration of such period) for an addi-

tional 2-year period upon a finding that the
relevant circumstances described in para-

graph (1) still exist. Any redesignation shall
be effective immediately following the end
of the prior 2-year designation or redesignation
period unless a different effective date is pro-

vided in such redesignation.”;

(8) paragraph (4)(C) by striking “(A)” and
inserting “(A)(ii)” after “paragraph (4)(B)”;

(9) in clause (i)—

(i) by inserting “or redesignation” after
“designation” the first place it appears; and

(ii) striking “of the designation”; and

(10) in clause (ii)—

(1) by striking “through (4)” and inserting
“and (3)”;

(2) by inserting at the end the following new
sentence: “Any revocation shall take ef-

fect on the date specified in the revocation
or upon publication in the Federal Register
if no effective date is specified.”;

(11) in paragraph (7), by inserting “, or the
revocation of a redesignation under para-

graph (6),” after “paragraph (5) or (6);” and

(i) CUSTODY.—The Attorney General shall

have custody of any alien who is certified

under paragraph (3).

(ii) RELEASE.—Except as provided in para-

graph (5), the Attorney General shall main-

tain custody of such an alien until the alien

is removed from the United States. Such cus-

tody shall be maintained irrespective of any

relief from removal for which the alien may

be eligible, or any relief from removal grant-

ed the alien, until the Attorney General de-

termines that the alien is no longer an alien

who may be certified under paragraph (3).

(iii) CERTIFICATION.—Any person in govern-

ment may certify an alien under this paragraph
if the Attorney General has reasonable grounds
to believe that the alien—


(A)(ii), or 237(a)(4)(B); or
“(B) is engaged in any other activity that endangers the national security of the United States.

“(4) NONDELETION.—The Attorney General may not delete an alien's record under paragraph (3) only to the Commissioner. The Commissioner may not delegate this authority.

“(5) JUDICIAL REVIEW OF PROCEEDINGS.—The Attorney General shall place an alien detained under paragraph (1) in removal proceedings, or shall charge the alien with a criminal offense, not later than 7 days after the commencement of such detention. If the requirement of the preceding sentence is not satisfied, the Attorney General shall release the alien.

“(b) HABEAS CORPUS AND JUDICIAL REVIEW.—Judicial review of any action or decision relating to this section (including judicial review of the merits of a determination described in subparagraph (A) or to deny visas to persons who would be inadmissible to the United States.

“3. TITLE IV—REMOVING OBSTACLES TO INVESTIGATING TERRORISM


“(a) SHORT TITLE.—This chapter may be cited as the “Professional Standards for Government Attorneys Act of 2001”.

“(b) PROFESSIONAL STANDARDS FOR GOVERNMENT ATTORNEYS.—

“(1) APPLICATION.—No violation of any disciplinary, ethical, or professional conduct rule shall be construed to preclude the inclusion of all reasonable evidence in any Federal criminal proceeding.

“(2) RULEMAKING AUTHORITY.—

“(A) In general.—The Attorney General shall make and amend rules of professional responsibility for Government attorneys.

“(B) Limitations.—

“1. TITLE V—INVESTIGATING TERRORISM

“SEC. 502. PROFESSIONAL STANDARDS FOR GOVERNMENT ATTORNEYS—CONTINUED.

“(a) DEFINITIONS.—In this section—

“(1) GOVERNMENT ATTORNEY.—The term ‘Government attorney’ means—

“(A) the Attorney General; the Deputy Attorney General; the Associate Attorney General; the head of, and any attorney employed in, any division, office, board, bureau, component, or agency (other than the Immigration and Nationality Office and the Attorney General) appointed by the Attorney General; any Assistant United States Attorney; any Special Assistant to the Attorney General or Special Attorney appointed under section 534 who is authorized to conduct criminal or civil law enforcement investigations or represent the United States; any other attorney employed by the Department of Justice who is authorized to conduct civil or criminal law enforcement investigations or represent the United States; any independent counsel, or employee of such counsel, appointed under chapter 40; and any outside special counsel, or employee of such counsel, who is duly appointed by the Attorney General;

“(B) the Secretary of State, in the Department of State, who is not authorized to represent the United States in criminal or civil law enforcement litigation or to supervise such proceedings;

“(C) the Attorney General or other law enforcement agent by the Attorney General;

“(D) recommendations with respect to actions or decisions of the court in or before which the proceeding is brought or is intended to be brought;

“(2) STATE.—The term ‘State’ includes a Territory and the District of Columbia.

“(3) CONSTRUCTION.—

“Subject to any uniform national rule prescribed by the Supreme Court under chapter 131, the standards of professional responsibility that apply to a Government attorney with respect to the attorney’s work for the Government shall be—

“(1) for conduct in connection with a grand jury proceeding, or conduct reasonably intended to lead to a grand jury proceeding, or conduct reasonably intended to lead to a grand jury proceeding, the standards of professional responsibility established by the rules and decisions of the court under whose authority the grand jury was or will be impaneled; and

“(2) for all other conduct, the standards of professional responsibility established by the rules and decisions of the Federal district court for the judicial district in which the attorney principally performs his or her official duties.

“(c) LICENSURE.—A Government attorney (except for foreign counsel employed in special cases)—

“(1) shall be duly licensed and authorized to practice as an attorney under the laws of a State; and

“(2) shall not be required to be a member of the bar of any particular State.

“(d) DISCOVERY.—Notwithstanding any provision of State law, including disciplinary rules, statutes, regulations, and constitutional provisions. The Government attorney may, for the purpose of enforcing Federal law, provide legal advice, authorization, concurrence, direction, or supervision of conduct, undercover activities, and any attorney employed as an investigator or other law enforcement agent by the Department of Justice who is not authorized to represent the United States in criminal or civil law enforcement litigation or to supervise such proceedings may participate in such activities, even though such activities may require the use of deceit or misrepresentation, where such activities are consistent with Federal law.

“(e) ADMISSIBILITY OF EVIDENCE.—No violation of any disciplinary, ethical, or professional conduct rule shall be construed to preclude the inclusion of all reasonable evidence in any Federal criminal proceeding.

“(f) RULEMAKING AUTHORITY.—The Attorney General shall make and amend rules of the Department of Justice to ensure compliance with this section.

“2. TITLE VI—CONFORMING AMENDMENT.


“(a) TITLE VI—CONFORMING AMENDMENT.—In order to encourage the Supreme Court to prescribe, under chapter 131 of title 28, United States Code, a uniform national rule for Government attorneys with respect to communications with represented persons and parties, not later than 1 year after the date of enactment of this Act, the Judicial Conference of the United States shall submit to the Chief Justice of the United States a report, which shall include recommendations with respect to amendments to the Federal Rules of Evidence and Procedure to provide for such a uniform national rule.

“(b) ACTUAL OR POTENTIAL CONFLICTS.—Not later than 2 years after the date of enactment of this Act, the Judicial Conference of the United States shall submit to the Chairmen and Ranking Members of the Committees on the Judiciary of the House of Representatives and the Senate a report, which shall include—

“(A) a review of any areas of actual or potential conflict between specific Federal duties related to the investigation and prosecution of violations of Federal law and the regulatory duties of Government attorneys (as that term is defined in section 530B of title 28, United States Code, as amended by this Act) by existing standards of professional responsibility;

“(B) recommendations with respect to amending the Federal Rules of Practice and Procedure to provide for additional rules governing the conduct of Government attorneys to address any areas of actual or potential conflict identified pursuant to the review under subparagraph (A).

“(c) IMPLEMENTATION.—In carrying out paragraphs (1) and (2), the Judicial Conference of the United States shall take into consideration—

“the needs and circumstances of multiforum and multijurisdictional litigations;
(B) the special needs and interests of the United States in investigating and prosecuting violations of Federal criminal and civil law; and
(C) that are approved under Federal statutory or case law or that are otherwise consistent with traditional Federal law enforcement techniques.

SEC. 502. ATTORNEY GENERAL'S AUTHORITY TO PAY REWARDS TO COMBAT TERRORISM.

(a) PAYMENT OF REWARDS TO COMBAT TERRORISM.—The Attorney General may be used for the payment of rewards pursuant to public advertisements for assistance to the Department of Justice to combat terrorism or defend the Nation against terrorist acts, in accordance with procedures and regulations established or issued by the Attorney General.

(b) CONDEMNORS.—In making rewards under this section—
(1) no such reward of $250,000 or more may be made or offered without the personal approval of either the Attorney General or the President; and
(2) the Attorney General shall give written notice to the Chairmen and ranking minority members of the Committee on Judiciary and the Committee of the House of Representatives not later than 30 days after the approval of a reward under paragraph (1).

(c) any executive agency or military department (as defined, respectively, in sections 105 and 102 of title 5, United States Code) may provide the Attorney General with funds for the payment of rewards;
(4) neither the failure of the Attorney General to authorize a payment nor the amount of a payment shall be subject to judicial review;
and
(5) no such reward shall be subject to any per- or aggregate reward spending limitation established by law, unless that law expressly refers to this section, and no reward paid pursuant to any such offer shall count toward any such aggregate reward spending limitation.

SEC. 503. SECRETARY OF STATE AUTHORITY TO PAY REWARDS.

Section 36 of the State Department Basic Authorities Act of 1994 (Public Law 103-563, August 1, 1996; 22 U.S.C. 2708) is amended—
(1) in subsection (b)—
(A) in paragraph (4), by striking “or” at the end and inserting “; or” after the second “or”;
(B) in paragraph (5), by striking the period at the end and inserting “; including by dismantling an organization in whole or significant part” after “or”; and
(C) by adding at the end the following:
“(6) the identification or location of an individual who holds a key leadership position in a terrorist organization;”; in a position not lower
(2) in subsection (d), by striking paragraphs (2) and (3) and redesignating paragraph (4) as paragraph (2); and
(3) in subsection (e), by inserting “, except as personally authorized by the Secretary of State if he determines that offer or payment of an award of a larger amount is necessary to combat terrorism or defend the Nation against terrorist acts;” after “$5,000,000”.

SEC. 504. DNA IDENTIFICATION OF TERRORISTS AND OTHER VIOLENT OFFENDERS.

Section 3(d)(2) of the DNA Analysis Backlog Elimination Act of 2000 (42 U.S.C. 1463a(d)(2)) is amended to read as follows:

“(2) The offenses described in paragraph (1), the following offenses shall be treated for purposes of this section as qualifying Federal offenses, as determined by the Attorney General:

(A) Any offense listed in section 2323(b)(5)(B) of title 18, United States Code.

(B) Any crime of violence (as defined in section 16 of title 18, United States Code).

(C) Any attempt or conspiracy to commit any of the above offenses.”.

SEC. 505. COORDINATION WITH LAW ENFORCEMENT.

(a) INFORMATION ACQUIRED FROM AN ELECTRONIC SURVEILLANCE.—Section 106 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806), is amended by adding at the end the following:

“(k) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against international terrorism.

“(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

“(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

“(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

“(2) Coordination authorized under paragraph (1) shall not preclude the certification requirement required by section 702 of title 50, United States Code, or the entry of an order under section 105.”.

(b) INFORMATION ACQUIRED FROM A PHYSICAL SEARCH.—Section 305 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1825) is amended by adding at the end the following:

“(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

“(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

“(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

“(2) Coordination authorized under paragraph (1) shall not preclude the certification requirements required by section 105 or the entry of an order under section 304.”.

SEC. 506. MISCELLANEOUS NATIONAL SECURITY AUTHORITIES.

(a) TELECOMMUNICATION AND TRANSACTIONAL RECORDS.—Section 2707(b) of title 18, United States Code, is amended—

(1) in the matter preceding paragraph (1), by inserting “or a Special Agent in Charge in a Bureau field office designated by the Director” after “Assistant Director”;

(2) in paragraph (1) before “(A)”, by inserting “(A)” in a position not lower

(A) by striking “in a position not lower than Deputy Assistant Director” and

(B) by striking “made that” and all that follows referring to “the Assistant Director”.

(b) CONSUMER REPORTS.

Section 624 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) in subsection (a) before “and”, by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “designee” the first place it appears;

and

(2) by striking “in writing that” and all that follows through the end and inserting the following: “in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”;

(c) CONGRESSIONAL RECORD

(1) in subsection (a) before “and”, by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “designee” the first place it appears;

and

(2) by striking “in writing that” and all that follows through the end and inserting the following: “in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”;

and

(3) in subsection (c) before “and”, by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “designee” the first place it appears; and

and

(4) by striking “in writing that” and all that follows through the end and inserting the following: “in camera that the consumer is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”.

SEC. 507. EXTENSION OF SECRET SERVICE JURISDICTION

(a) CONCURRENT JURISDICTION UNDER 18 U.S.C. 1030.—Section 1030(d)(1) of title 18, United States Code, is amended to read as follows:

“(d)(1) The United States Secret Service shall, in addition to any other agency having jurisdiction under...
such authority, have the authority to investigate offenses under this section.

"(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses described in subsection (a)(1) for any case involving espionage, foreign counterintelligence, information protected against unauthorized disclosure by any Federal law or by any agreement entered into by the United States and any foreign country, or Restricted Data (as that term is defined in section 11 of the Atomic Energy Act of 1946 (42 U.S.C. 1921)) if the Director believes that the handling, transfer, receipt, or possession of such data is a violation of subsection (a)(3).

"(b) The Attorney General, in consultation with the Secretary of Defense, the Director of Central Intelligence, and the heads of such other Federal agencies as the Attorney General may designate, may submit a written application to a court of competent jurisdiction for an ex parte order requiring the production of any document or other article in the possession of the United States, or an agency or instrumentality of the United States, if the Attorney General believes that the production of such document or other article is likely to contain information described in paragraphs (1) and (3) of such section

"(1) to a court order under this subsection.

"(2) The court shall issue an order describing the document or article referred to in paragraph (1) if the court finds that the application for the order includes a certification described in subparagraph (A), and that the application was submitted to the Attorney General (or his designee) to—

"(A) collect reports, records, and information (including individually identifiable information) in the possession of the Attorney General or any other Federal agency or instrumentality that are relevant to an investigation or prosecution of an offense listed in section 2332d(g)(5)(B) of title 18, United States Code, or an act of domestic or international terrorism as defined in section 2331 of that title; and

"(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such records, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

"(2) The Attorney General (or his designee) shall—

"(A) in general.—An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the information sought is described in paragraph (1)(A).

"(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

"(C) PROTECTION.—An officer or employee of the Department who, in good faith, produces information in accordance with an order issued under this subsection does not violate subsection (b)(2) and shall not be liable to any person for that production.

TITLE VI—PROVIDING FOR VICTIMS OF TERRORISM, PUBLIC SAFETY OFFICERS, AND THEIR FAMILIES

Subtitle A—Aid to Families of Public Safety Officers

SEC. 610. TECHNICAL CORRECTION WITH RESPECT TO HUMILITY OF HEROIC PUBLIC SAFETY OFFICERS.

"(a) Payments.—Section 1201(a) of the Omnibus Crime Control and Safe Streets Act of 1990 (42 U.S.C. 13971) is amended by striking "$100,000" and inserting "$250,000.

Subtitle B—Amendments to the Victims of Crime Act of 1984

SEC. 611. EXPEDITED PAYMENT FOR PUBLIC SAFETY OFFICERS INVOLVED IN THE PREVENTION, INVESTIGATION, RESOLUTION, OR PROSECUTION OF OFFENSES RELATED TO A TERRORIST ATTACK.

"(a) In General.—Notwithstanding the limitations described in section 1201 of the provisions of subsections (c), (d), and (e) of such section or section 1202 of title I of the Omnibus Crime Control and Safe Streets Act of 1990 (42 U.S.C. 13961, 1396a), upon certification (containing identification of all eligible payees pursuant to section 1201 of such Act) by a public agency that a public safety officer was killed or suffered a catastrophic injury producing permanent and total disability occurring on or after January 1, 2001, the Director shall distribute amounts from the Fund in the previous fiscal year, except the amount distributed in the previous fiscal year is more than 2 times the amount distributed in the previous fiscal year, and the amount distributed in the previous fiscal year is more than 2 times the amount distributed in the previous fiscal year.

"(b) Certification.—The certification described in subsection (a) shall apply to any death or disability occurring on or after January 1, 2001.

SEC. 612. TECHNICAL CORRECTION WITH RESPECT TO HUMILITY OF HEROIC PUBLIC SAFETY OFFICERS.

"(a) Payments.—Section 103 of the Omnibus Crime Control and Safe Streets Act of 1990 (42 U.S.C. 13971) is amended by striking "$100,000" and inserting "$250,000.

"(b) Formula for Fund Distributions.—Section 1202(c) of the Victims of Crime Act of 1984 (42 U.S.C. 16061(c)) is amended to read as follows:

"(1) the amount distributed in a fiscal year that the amount distributed in the previous fiscal year is more than 2 times the amount distributed in the previous fiscal year.

"(2) In each fiscal year, the Director shall distribute amounts from the Fund in accordance with subsection (d). All sums not distributed during a fiscal year shall remain in reserve in the Fund to be distributed during subsequent fiscal years. In distributing the amount of any other provision of law, all sums deposited in the Fund that are not distributed
shall remain in reserve in the Fund for obliga-
tions from amounts deposited to or
available in the Fund, not-
to provide compensation to victims of
terrorist acts that occurred on September 11,
2001, as an antiterrorism emergency reserve.

3. The antiterrorism emergency reserve
carried forward from the fiscal year 2001,
and any such amounts carried over from the
capital reserve established pursuant to sub-
section (c) and section 619 of the Depart-
ment of Commerce, Justice, and State, the
Emergency reserve established pursuant to sub-
section (A) may be carried over from fis-
ical year to fiscal year after distributing amounts under
paragraphs (2), (3) and (4). Such reserve shall not
be less than $100,000,000.

4. (a) The antiterrorism emergency reserve
referred to in subparagraph (A) may be used for
supplemental grants under section 1404B and
to provide compensation to victims of international terrorism under section 1404C.

(b) Amounts in the antiterrorism emer-
gency reserve established pursuant to sub-
paragraph (A) shall be carried over from one
fiscal year to the next fiscal year. Notwithstanding sub-
section (c) and section 619 of the Depart-
ments of Commerce, Justice, and State, the
Judicial and Related Agencies Appropriations Act, 2001, and any similar limitation on Fund obligations in any future Act, un-
less the same shall expressly refer to this section, any such amounts carried over shall not be subject to any limitation on ob-
ligations from amounts deposited to or
available in the Fund.

—Victims of Crime Act of 1984.—
Amounts transferred to the Crime Victims
Fund for use in responding to the airplane hijackings and
terrorist acts that occurred on September 11,
2001, shall not be subject to any limitation on ob-
ligations from amounts deposited to or
available in the Fund.

SEC. 622. CRIME VICTIM COMPENSATION.

(a) Allocation of Funds for Compensation
and Assistance.—Paragraphs (1) and (2)
of section 1403(a) of the Victims of Crime Act of
1984 (42 U.S.C. 10602(a)) are amended by in-
serting “in fiscal year 2002 and of 60 percent in
subsequent fiscal years” after “40 percent”.

(b) Location of Compensable Crime.—Section
1403(b)(6)(B) of the Victims of Crime Act of
1984 (42 U.S.C. 10602(b)(6)(B)) is amended by
inserting “are outside the United States (if
the compensable crime is terrorism, as de-
fined in section 2351 of title 18) or”.

(c) Amendment of Crime Victim Com-
ensation to Means-Tested Federal Bene-
fit Programs.—Section 1403 of the Victims
of Crime Act of 1984 (42 U.S.C. 10602) is
amended by striking subsection (c) and in-
serting the following:

(c) Exclusion From Income, Resources,
and Means Tests.—Notwithstanding any other law
(other than title IV of Public Law 107-42, for the
purpose of any maximum allowed income
eligibility requirement in any Federal, State, or local
government program using Federal funds that pro-
vides medical or other assistance (or pay-
s for the purpose of such assistance), any amount of crime victim
compensation that the applicant receives through a crime victim compensation pro-
gram under this subsection shall not be included in the
income, resources, or assets of the appli-
cant, nor shall that amount reduce the
amount of the assistance available to the
applicant from Federal, State, or local
government programs using Federal funds, unless the
total amount of assistance that the applicant
receives from such programs is sufficient to fully compensate the applicant for
losses suffered as a result of the crime.

(d) Definitions of “Compensable Crime”
and “State”.—Section 1403(d) of the Victims
of Crime Act of 1984 (42 U.S.C. 10602(d)) is
amended—

(1) in paragraph (3), by striking “crimes in-
volving terrorism,” and
(2) in paragraph (4), by inserting “the United
States Virgin Islands,” after “the
Commonwealth of Puerto Rico.”.

(e) Relationship of Eligible Crime Victim
Compensation Programs to the September
11th Victim Compensation Fund.—

(1) In General.—Section 1403(e) of the Vic-
tems of Crime Act of 1984 (42 U.S.C. 10602(e))
is amended by striking “other than the pro-
gram established under title IV of Public
Law 107-42,” after “Federal program,”.

(2) Compensation.—With respect to any
compensation program established under title IV of Pub-
lic Law 107-42, the failure of a crime victim
compensation program, after the effective
date of final regulations issued pursuant to
paragraph (4), to provide compensation otherwise required pursuant to
section 1403 of the Victims of Crime Act of
1984 (42 U.S.C. 10602) shall render that
program ineligible for future grants under

SEC. 623. CRIME VICTIM ASSISTANCE.

(a) Assistance for Victims in the Dis-
tricts of Columbia and Other Territories
and Possessions.—Section 1404(a) of the Victims of Crime Act of
1984 (42 U.S.C. 10604(a)) is amended by adding at the end the following:

“(6) An agency of the Federal Government
performing local law enforcement functions in
and on behalf of the District of Columbia, the
Commonwealth of Puerto Rico, the
United States Virgin Islands, or any other
territory or possession of the United States
may qualify as an eligible crime victim as-
sistance program for the purpose of grants
under this subsection, or for the purpose of
grants under subsection (c)(1).”.

(b) Prohibition on Discrimination Against
Certain Victims.—Section 1404(b)(1) of the
Victims of Crime Act of 1984 (42 U.S.C.
10604(b)(1)) is amended—

(1) in subparagraph (D), by striking “and” at the end;

(2) in subparagraph (E), by striking the pe-
riod at the end and inserting “; and”;

(3) by adding at the end the following:

“(P) discrimination against victims because
they disagree with the way the
State is prosecuting the criminal case.”.

(c) Grants for Program Evaluation and
Compendium.—Section 1404(c)(1)(A) of the Victims of Crime Act of
1984 (42 U.S.C. 10604(c)(1)(A)) is amended by inserting “, pro-
gram evaluation, compliance efforts,” after “demonstration projects”.

(d) Allocation of Discretionary
Grants.—Section 1404(b)(2) of the Victims
of Crime Act of 1984 (42 U.S.C. 10604(b)(2)) is amended—

(1) in subparagraph (A), by striking “not
more than” and inserting “not less than”;

(2) in subparagraph (B), by striking “not
less than” and inserting “not more than”.

(e) Fellowships and Clinical Intern-
ts.—Section 1404(c)(3) of the Victims
of Crime Act of 1984 (42 U.S.C. 10604(c)(3)) is amended—

(1) in subparagraph (C), by striking “and” at the end;

(2) in subparagraph (D), by striking the pe-
riod at the end and inserting “; and”;

(3) by adding at the end the following:

“(E) use funds made available to the Direc-
tor under this subsection—

“(i) for fellowships and clinical intern-
ships; and

“(ii) to carry out programs of training and
special workshops for the presentation and
dissemination of information resulting from
emonstrations, surveys, and special

SEC. 624. VICTIMS OF TERRORISM.

(a) Compensation and Assistance to Vic-
tims of Domestic Terrorism.—Section
1404(b)(5) of the Victims of the Crime Act of 1984
(42 U.S.C. 10604(b)(5)) is amended to read as follows:

“(b) Victims of Terrorism Within the
United States.—The Director may make
supplemental grants as provided in section
1402(d)(5) to States for eligible crime victim
compensation and assistance programs, and
to public and service organizations, public agen-
cies (including Federal, State, or local gov-
ernments) and nongovernmental organiza-
tions that provide assistance to victims of
terrorism and that may be used to provide emer-
gency relief, including crisis response ef-
forts, assistance, compensation, training and
technical assistance, and ongoing assistance,
including during any investigation or pros-
ection, to victims of terrorist acts or mass
violence occurring within the United States.

(b) Assistance to Victims of Inter-
national Terrorism.—Section 1404(b)(1) of the Victims of Crime Act of 1984 (42 U.S.C. 10604(b)(1)) is amended by striking “who are eligible for assistance
under title VIII of the Omnibus Diplomatic Secu-
rit and Antiterrorism Act of 1986”.

(c) Compensation to Victims of Inter-
national Terrorism.—The Director may make
supplemental grants as provided in section
1402(d)(5) to States for eligible crime victim
compensation and assistance programs, and
to public and service organizations, public agen-
cies (including Federal, State, or local gov-
ernments) and nongovernmental organiza-
tions that provide assistance to victims of
terrorism and that may be used to provide emer-
gency relief, including crisis response ef-
forts, assistance, compensation, training and
technical assistance, and ongoing assistance,
including during any investigation or pros-
ection, to victims of terrorist acts or mass
violence occurring within the United States.

TITLE VII—INCREASED INFORMATION
SHARING FOR CRITICAL INFRASTRUCTURE
PROTECTION

SEC. 711. EXPANSION OF REGIONAL INFORMA-
TION SHARING SYSTEM TO FACILI-
TATE FEDERAL-STATE-LOCAL LAW
ENFORCEMENT RESPONSE RELATED TO TERRORIST ATTACKS.

Section 1001 of title I of the Omnibus Crime Control and Safe Streets Act of 1968
(42 U.S.C. 20703) is amended—

(1) in subsection (a), by inserting “and ter-
orror conspiracies and activities” after “ac-
ivities”;

(2) in subsection (b), by inserting “Amend-
ded” after the semicolon.
(B) by redesigning paragraph (4) as paragraph (5);  
(C) by inserting after paragraph (3) the following:

"14. establishing and operating secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing transnational terrorist conspiracies and activities; and (5);"; and

(3) by inserting at the end the following:

"(d) of Appropriation to the Bureau of Justice Assistance.—There are authorized to be appropriated to the Bureau of Justice Assistance to carry out this section $95,000 for fiscal year 2002 and $100,000,000 for fiscal year 2003."

Title VIII—Strengthening the Criminal Laws Against Terrorism

Section 801. Terrorist Attacks and Other Acts of Violence Against Mass Transportation Systems

Chapter 97 of title 18, United States Code, is amended by adding at the end the following:

"§ 993. Terrorist attacks and other acts of violence against mass transportation systems

(a) General Prohibitions.—Whoever willfully:

"(1) wrecks, derails, sets fire to, or disables a mass transportation vehicle or ferry;

"(2) places or causes to be placed, runs, or otherwise makes available or transfers any biological agent or toxin for use as a weapon, destructive substance, or destructive device in, upon, or near a mass transportation vehicle or any mass transportation facility, with intent to endanger the safety of any passenger or employee of the mass transportation provider, or with a reckless disregard for the safety of human life;

"(3) sets fire to, or places any biological agent or toxin for use as a weapon, destructive substance, or destructive device in, upon, or near any garage, terminal, structure, supply, or facility used in the operation of, or in support of the operation of, a mass transportation vehicle or ferry, without previously obtaining the permission of the mass transportation provider, and knowing or having reason to know such activity would likely derail, disable, or wreck a mass transportation vehicle or ferry used, operated, or employed by the mass transportation provider;

"(4) removes appurtenances from, damages, or otherwise impedes the operation of a mass transportation vehicle or ferry, with intent to endanger the safety of any passenger or employee of the mass transportation provider, or with a reckless disregard for the safety of human life;

"(5) interferes with, disables, or incapacitates any dispatcher, driver, captain, or person while they are employed in dispatching, operating, or maintaining a mass transportation vehicle or ferry, with intent to endanger the safety of any passenger or employee of the mass transportation provider, or with a reckless disregard for the safety of human life;

"(6) commits an act, including the use of a dangerous weapon, with the intent to cause death, bodily injury to any person other than an employee or passenger of a mass transportation provider or any other person while any of the foregoing are on the property of a mass transportation provider, with intent to endanger the safety of any passenger or employee of a mass transportation provider, or with a reckless disregard for the safety of human life;

"(7) transmits or causes to be transmitted false information, knowing the information to be false, concerning an attack or alleged attack or to be made, to any act which would be unlawful prohibited by this subsection; or

"(8) attempts, threatens, or conspires to do any of the foregoing, shall be fined under this title or imprisoned not more than twenty years, or both, if such act is committed, or in the case of a threat or conspiracy such act would be committed, on, against, or affecting a mass transportation provider engaged in or affecting interstate commerce, or on the course of committing such act, that person travels or communicates across a State line in order to commit such act, or transports materials necessary to commit such act, across a State line in aid of the commission of such act.

(b) Aggravated Offense.—Whoever commits an offense under subsection (a) in a circumstance in which that person travels or communicates across a State line in order to commit such act, or transports materials necessary to commit such act, across a State line in aid of the commission of such act, shall be guilty of an aggravated form of the offense and shall be fined under this title or imprisoned for a term of years or for life, or both.

(c) Definitions.—In this section—

"(1) the term ‘biological agent’ has the meaning given to that term in section 178(1) of this title;

"(2) the term ‘dangerous weapon’ has the meaning given to that term in section 930 of this title;

"(3) the term ‘destructive device’ has the meaning given to that term in section 922(a)(4) of this title;

"(4) the term ‘destructive substance’ has the meaning given to that term in section 31 of this title;

"(5) the term ‘mass transportation’ has the meaning given to that term in section 592a(a) of title 49, United States Code, except that the term shall include schoolbus, charter, and sightseeing transportation;

"(6) the term ‘serious bodily injury’ has the meaning given to that term in section 1365 of this title;

"(7) the term ‘State’ has the meaning given to that term in section 2366 of this title; and

"(8) the term ‘toxin’ has the meaning given to that term in section 178(2) of this title.

(f) Conforming Amendment.—The analysis of chapter 97 of title 18, United States Code, is amended by adding at the end:

"1993. Terrorist attacks and other acts of violence against mass transportation systems.

Section 802. Expansion of the Biological Weapons Statute

Chapter 10 of title 18, United States Code, is amended—

(1) in section 175—

(a) in subsection (b)—

(i) by striking ‘‘does not include’’ and inserting ‘‘includes’’;

(ii) by inserting ‘‘other than’’ after ‘‘system for’’; and

(iii) by inserting ‘‘bona fide research’’ after ‘‘protective’’;

(b) by redesignating subsection (b) as subsection (c); and

(c) by inserting after subsection (a) the following:

"(b) Additional Offense.—Whoever knowingly possesses any biological agent, toxin, or destructive substance of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose, shall be fined under this title, imprisoned not more than 10 years, or both. In this subsection, the term ‘biological agent’ and ‘toxin’ do not encompass any biological agent or toxin that is in its naturally-occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source.

(2) by inserting after section 175a the following:

"SEC. 175b. Possession by Restricted Persons.

"(a) No restricted person described in subsection (b) shall ship or transport interstate or foreign commerce, or in or affecting interstate or foreign commerce, any destructive substance, any biological agent or toxin, or receive any biological agent or toxin that has been shipped or transported in interstate or foreign commerce, if the biological agent or toxin is listed as a select agent in subsection (j) of section 72.6 of title 42, Code of Federal Regulations, pursuant to section 513(a)(1) of the Anti-Terrorism and Effective Death Penalty Act of 1996 (Public Law 104–132), and is not exempted under subsection (b) of section 72.8, or appendix A of part 72 of the Code of Regulations.

"(b) In this section—

"(1) The term ‘select agent’ does not include any such biological agent or toxin that is in its naturally-occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source.

"(2) The term ‘restricted person’ means an individual who—

"(A) is under indictment for a crime punishable by imprisonment for a term exceeding 1 year;

"(B) has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year;

"(C) is a fugitive from justice;

"(D) is an alien unlawfully or illegally in the United States;

"(F) has been adjudicated as a mental deforesee or has been committed to any mental institution;

"(G) is an alien (other than an alien lawfully admitted for permanent residence) who is not a national of a country with which the Secretary of State, pursuant to section 6(j) of the Export Administration Act of 1979 (50 U.S.C. App. 2405(j)), section 623A of chapter 1 of part M of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), or section 40(d) of chapter 3 of the Armas Export Control Act (22 U.S.C. 2780(d)), has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism; or

"(H) has been discharged from the Armed Services of the United States under dishonorable conditions.

"(3) The term ‘alien’ has the same meaning as in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)).

"(4) The term ‘lawfully admitted for permanent residence’ has the same meaning as in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(20)).

"(c) Whoever knowingly violates this section shall be fined as provided in this title, imprisoned not more than 10 years, or both; but the prohibition contained in this section shall not apply with respect to any duly authorized United States governmental activity.

and

3. in the chapter analysis, by inserting after the item relating to section 175a the following:

"175b. Possession by restricted persons.

Section 803. Definition of Domestic Terrorism

As used in this chapter, the term ‘Domestic Terrorism’—

(1) in paragraph (1)(B)(ii), by striking ‘‘by assassination or kidnapping’’ and inserting ‘‘by mass destruction, assassination, or kidnaping’’;

(2) in paragraph (5), by striking ‘‘and’’;

(3) in paragraph (4), by striking the period at the end and inserting ‘‘;’’; and

(4) by adding at the end the following:

"§ 803. Definition of Domestic Terrorism.

As used in this chapter, the term ‘Domestic Terrorism’—

(1) includes—
“(d) To influence the policy of a government by intimidation or coercion; or

“(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.”

“(C) occur primarily within the territorial jurisdiction of the United States.”

(b) CONFORMING AMENDMENT.—Section 3077(d)(1) of the United States Code, is amended to read as follows:

“(1) ‘act of terrorism’ means an act of domestic or international terrorism as defined in section 2339A(a).”

SEC. 804. PROHIBITION AGAINST HARBORING TERRORISTS.

(a) In General.—Chapter 113B of title 18, United States Code, is amended by adding after section 2338 the following new section:

“§ 2339. Harbecing or concealing terrorists

“(a) Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe, has committed, or is about to commit, an offense under section 32 (relating to destruction of aircraft or aircraft facilities), section 2338 (relating to terrorism transcending national boundaries), section 2339 (relating to harboring terrorists), section 2332a (relating to weapons of mass destruction), paragraph (2) or (3) of section 844(f) (relating to arson and bombing of government property risking or causing injury or death), section 1366(a) (relating to the destruction of an energy facility), section 2300 (relating to violence against maritime navigation), section 2332a (relating to weapons of mass destruction), or section 2332b (relating to acts of terrorism transcending national boundaries) of this title, section 236(a) (relating to acts of terrorism transcending national boundaries), or section 236(b) (relating to acts of terrorism transcending national boundaries), or section 236(c) (relating to acts of terrorism transcending national boundaries), or section 236(d) (relating to Presidential and Presidential staff assassination and kidnaping), or section 236(e) (relating to assassination and kidnaping), 351 (a) through (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1116 (relating to murder or attempted murder of other than U.S. citizens or residents of the United States, citizens or residents of the United States, or their property, or all persons engaged in an activity affecting the United States, citizens or residents of the United States, or their property, or all persons engaged in an activity affecting the United States, citizens or residents of the United States, or their property), paragraph (2) or (3) of section 844(f) (relating to arson and bombing of government property risking or causing injury or death), section 1366(a) (relating to the destruction of an energy facility), section 2300 (relating to violence against maritime navigation), section 2332a (relating to weapons of mass destruction), section 2332b (relating to acts of terrorism transcending national boundaries), section 2339 (relating to harboring terrorists), section 2339A (relating to providing material support to terrorists), section 2339B (relating to providing material support to terrorist organizations), or section 2404A (relating to torture) of this title;

“(ii) section 2338 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2292(a)), or section 46502 (relating to aircraft piracy) of title 49, shall be fined under this title or imprisoned not more than ten years, or both.”

“(b) A violation of this section may be prosecuted at any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.”

(b) TECHNICAL AMENDMENT.—The chapter analysis for chapter 113B of title 18, United States Code, is amended by inserting after the item for section 2338 the following:

“2339. Harbecing or concealing terrorists.”

SEC. 805. JURISDICTION OVER CRIMES COMMITTED AT U.S. FACILITIES ABROAD.

Section 7 of title 18, United States Code, is amended by adding at the end the following:

“(9) With respect to offenses committed by or against a United States national as defined in section 1233(c) of this title—

“(A) the premises of United States diplomatic, consular, military or other United States Government missions or entities in foreign States, including the buildings, parts of buildings, and land appurtenant or ancillary thereto or used for purposes of those missions or entities, irrespective of ownership; and

“(B) residences in foreign States and the land appurtenant or ancillary thereto, irrespective of ownership, used for purposes of those missions or entities or used by United States personnel assigned to those missions or entities.

Nothing in this paragraph shall be deemed to supersede any treaty or international agreement or any provision of United States law analogous to any provision listed in section 2332b(g)(5)(B) other than a provision listed in section 2329, or a violation of section 112, 351(e), 1361, or 1366(a) of this title, or section 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed.”

SEC. 806. MATERIAL SUPPORT FOR TERRORISM.

(a) In General.—Section 2339A of title 18, United States Code, is amended—

“(1) in subsection (a) (by inserting after “within the United States,” ‘‘or both’’); and

“(2) in subsection (b) (by inserting after ‘‘2339A’’ ‘‘or both’’).”

SEC. 807. ASSETS OF TERRORIST ORGANIZATIONS.

Section 581(a)(1) of title 18, United States Code, is amended by inserting at the end the following:

“§ 581. Security of interests in property

“(a)(1)(A) All assets, foreign or domestic—

“(i) of any person, entity, or organization engaged in planning or perpetrating any act of domestic or international terrorism (as defined in section 2331), against the United States, citizens or residents of the United States, or their property, or all persons engaged in an activity affecting the United States, citizens or residents of the United States, or their property;

“(ii) acquired or maintained by any person for the purpose of supporting, planning, conducting, or concealing an act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property;

“(iii) derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property;”

Sec. 808. TECHNICAL CLARIFICATION RELATING TO PROHIBITION OF MATERIAL SUPPORT TO TERRORISM.

No provision of the Trade Sanctions Reform and Export Enhancement Act of 2000 (title IX of Public Law 106-387) shall be construed to limit or otherwise affect section 2339A or 2339B of title 18, United States Code.

SEC. 809. DEFINITION OF FEDERAL CRIME OF TERRORISM.

Section 2332b of title 18, United States Code, is amended—

“(1) in subsection (d) (by inserting after “2338” ‘‘or both’’); and

“(2) in subsection (g)(5)(B) (by striking clauses (1) through (3) and inserting the following:

“(i) section 2332 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to terrorism by means of a chemical weapon), 351 (a) through (d) (relating to congressional, cabinet, and Supreme Court jurisdiction of the United States), 841(m) or (n) (relating to nuclear materials), 841(f) (2) through (3) (relating to aircraft piracy), section 1136 (relating to bombing of Government property or possessing or carrying)(relating to terrorism by means of a chemical weapon), section 1136 (relating to bombing of property used in interstate commerce), section 1193 (relating to attempting or attempted attack on Federal facilities or property), paragraph (5)(A)(i) resulting in damage as defined in 1193(b)(5)(B)(ii), (iii) (relating to computer, 1114 (relating to terrorism by means of a chemical weapon), 351 (a) through (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to protection of Presidential and Presidential staff assassination and kidnaping), 1993 (relating to terrorism by means of a chemical weapon), 351 (a) through (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1994 (relating to terrorism by means of a chemical weapon), 351 (a) through (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1995 (relating to terrorism by means of a chemical weapon), 351 (a) through (d) (relating to Presidential and Presidential staff assassination and kidnaping), or other than a violation of section 2332b(g)(5)(B) other than a provision listed in section 2329, or a provision listed in section 112, 351(e), 1361, or 1366(a) of this title, or section 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed.”

SEC. 810. NO STATUTE OF LIMITATION FOR CERTAIN TERRORISM OFFENSES.

(a) General.—Section 3286 of title 18, United States Code, is amended to read as follows:

“§ 3286. Extension of statute of limitation for certain terrorism offenses.

“(a) EIGHT-YEAR LIMITATION.—Notwithstanding section 3282, no person shall be prosecuted, tried, or punished for any non-capital offense involving any provision listed in section 2332b(g)(5)(B) other than a provision listed in section 2329, or a violation of section 112, 351(e), 1361, or 1366(a) of this title, or section 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed.”

Sec. 811. LIMITATION.—Notwithstanding any other law, an indictment may be found or an information instituted at any time without regard to the 8 year limitation provisions of section 2332b(g)(5)(B), if the commission of such offense resulted in, or created a foreseeable risk of assassination and kidnaping.”
of, death or serious bodily injury to another person.”

(b) APPLICATION.—The amendments made by this section shall apply to the prosecution of any attempt or conspiracy before, on, or after the date of enactment of this section.

SEC. 811. ALTERNATE MAXIMUM PENALTIES FOR SELECTED OFFENSES.

(a) ARSON.—Section 81 of title 18, United States Code, is amended in the second undersigned paragraph by striking “not more than twenty years” and inserting “for any term of years or for life”.

(b) DESTRUCTION OF AN ENERGY FACILITY.—Section 1396 of title 18, United States Code, is amended—

(1) in subsection (a), by striking “ten” and inserting “twenty”;

(2) by striking “and inserting ‘twenty’;” and

(3) in the third sentence, by striking “and inserting any” and inserting “and inserting ‘any’”.

(c) MURDER.—Section 1113 of title 18, United States Code, is amended—

(1) by striking “and, if the death of any person results, shall be imprisoned for any term of years or for life.”;

(d) MURDER OF A JUDGE OR MAGISTRATE.—Section 1114 of title 18, United States Code, is amended—

(1) by striking “and, if the death of any person results, shall be imprisoned for any term of years or for life.”;

(e) MURDER BY A CLANSMAN.—Section 1115 of title 18, United States Code, is amended—

(1) by striking “and, if the death of any person results, shall be imprisoned for any term of years or for life.”;

(f) MURDER IN VIOLATION OF LAW.—Section 1116 of title 18, United States Code, is amended—

(1) by striking “and, if the death of any person results, shall be imprisoned for any term of years or for life.”;

SEC. 812. PENALTIES FOR TERRORIST CONSPIRACIES.

(a) ARSON.—Section 81 of title 18, United States Code, is amended in the first undersigned paragraph—

(1) by striking “or, attempts to set fire to or burn”;

(2) by inserting “or attempts or conspires to do such an act,” before “shall be imprisoned”;

(b) KILLINGS IN FEDERAL FACILITIES.—

(1) Section 930(c) of title 18, United States Code, is amended—

(A) by striking “or attempts to kill”;

(B) by inserting “or attempts or conspires to do such an act,” before “shall be punished”;

(C) by striking “and 1113” and inserting “1112, and 1113”;

(2) Section 1117 of title 18, United States Code, is amended by inserting “930(c),” after “section”.

(c) COMMUNICATIONS LINES, STATIONS, OR SYSTEMS.—Section 1362 of title 18, United States Code, is amended in the first undersigned paragraph—

(1) by striking “or attempts willfully or maliciously to injure or destroy”;

(2) by inserting “or attempts or conspires to do such an act,” before “shall be fined”; and

(d) BUILDINGS OR PROPERTY WITHIN SPECIAL MARITIME AND TERRITORIAL JURISDICTION.—

Section 1363 of title 18, United States Code, is amended—

(1) by striking “or attempts to destroy or injure”; and

(2) by inserting “or attempts or conspires to do such an act,” before “shall be fined”.

(e) WRECKING TRAINS.—Section 1992 of title 18, United States Code, is amended by adding at the end the following:

“(c) CONSPIRACY.—A person who conspires to commit an offense under this section shall be subject to the same penalties (other than the penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy.”

(f) MURDER.—Section 1993 of title 18, United States Code, is amended by inserting “or attempts or conspires to do such an act,” before “shall be fined”.

(g) TERRORISM.—Section 1994 of title 18, United States Code, is amended by adding at the end the following:

“(c) CONSPIRACY.—A person who conspires to commit an offense under this section shall be subject to the same penalties (other than the penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy.”

(h) SABOTAGE OF NUCLEAR FACILITIES OR FUEL.—Section 238(a)(5) of title 18, United States Code, is amended—

(1) by striking “and inserting ‘and’;

(2) by striking the period at end and inserting “; and”;

(i) INJURY TO OR DESTRUCTION OF POWER FACILITIES.—Section 1961(1) of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) by striking “or”, who intentionally and willfully attempts to destroy or cause physical damage;

(B) in paragraph (4), by striking the period at the end and inserting a comma; and

(C) by striking “or attempts or conspires to do such an act,” before “shall be fined”;

(2) in subsection (b)—

(A) by striking “or attempts to cause”;

(B) by inserting “or attempts or conspires to do such an act,” before “shall be fined”;

(C) by inserting “or attempts or conspires to do such an act,” before “shall be fined”;

(3) in subsection (c)—

(A) by striking “or, who intentionally and willfully attempts to destroy or cause physical damage”;

(b) ‘‘SABOTAGE OF NUCLEAR FACILITIES OR FUEL.—Section 238(a)(5) of title 18, United States Code, is amended—

(1) in paragraph (a)—

(A) by striking “as provided in subsection (b),” before “a fine”;

(B) by inserting “(a)(5)(A)” and inserting “(a)(5)(A)(iii)”;

(ii) physical injury to any person;

(iii) a threat to public health or safety; or

(iv) damage affecting a computer system used by or for a Government entity in furtherance of the administration of justice, national defense, or national security.”;

(b) PENALTIES.—Section 1960(c) of title 18, United States Code is amended—

(1) in paragraph (2)—

(A) by striking “in the case of an offense punishable under this subparagraph, after “subsection (a)”, in the matter preceding clause (i), and

(B) in clause (i), by striking “and” and inserting “; and”;

(c) and inserting “(a)(5)(A)(iii)”;

(d) by striking “and” at the end;

(2) in paragraph (3)—

(A) by striking “(a)(5)(A), (a)(5)(B),” both places it appears; and

(B) by striking “and” at the end;

(3) by striking “(a)(5)(C)” and inserting “(a)(5)(A)(iii)”;

(e) CONSPIRACY.—If two or more persons conspire to violate subsection (b) or (c), and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in such subsection.”

(k) DAMAGING OR DESTROYING AN INTERSTATE PIPELINE FACILITY.—Section 46505(b) of title 49, United States Code, is amended—

(1) by striking “or attempting to damage or destroy;”;

(2) by inserting “, or attempting or conspiring to do such an act,” before “shall be punished”;

SEC. 813. POST-RELEASE SUPERVISION OF TERRORISTS.

Section 3358 of title 18, United States Code, is amended by adding at the end the following:

“(j) SUPERVISED RELEASE TERMS FOR TERRORIST PREREQUISITES.—Notwithstanding subsection (b), the authorized term of supervised release for any offense listed in section 2322(g)(5)(B), the commission of which resulted in, or created a foreseeable risk of, death or serious bodily injury to another person, is any term of years or life.”

SEC. 814. INCLUSION OF ACTS OF TERRORISM AS RACKETEERING ACTIVITY.

Section 1961(c) of title 18, United States Code, is amended—

(1) by striking “or (F)” and inserting “(F);” and

(2) by inserting before the semicolon at the end the following: “; or (G) any act that is indictable as an offense listed in section 2322(g)(5)(B)”.

SEC. 815. DETERRENCE AND PREVENTION OF CYBER TERRORISM.

(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS.—Section 1833(a)(5) of title 18, United States Code, is amended—

(1) by inserting “(i)” after “A”;

(2) by redesignating paragraphs (B) and (C) as clauses (i) and (ii), respectively;

(3) by adding “and” at the end of clause (iii), as so redesignated; and

(4) by adding at the end the following:

“(B) caused (or, in the case of an attempted offense, would, if completed, have caused) conduct described in clause (i), (ii), or (iii) of subparagraph (A) that resulted in—

(1) loss to 1 or more persons during any 1-year period (including resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(2) material destruction or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, care of, or more individuals;

(3) physical injury to any person;

(4) a threat to public health or safety; or

(5) damage affecting a computer system used by or for a Government entity in furtherance of the administration of justice, national defense, or national security.”;

(b) PENALTIES.—Section 1030(c) of title 18, United States Code is amended—

(1) in paragraph (2)—

(A) by striking “in paragraph (A)” —

(i) by inserting “except as provided in subparagraph (B),” before “a fine”;

(ii) by inserting “(a)(5)(A)” and inserting “(a)(5)(A)(iii)”;

(iii) by striking “and” at the end;

(B) in subparagraph (B), by inserting “an attempt to commit an offense punishable under this subparagraph, after “subsection (a)”, in the matter preceding clause (i), and

(C) in subparagraph (C), by striking “and” at the end;

(2) in paragraph (3)—

(A) by striking “, (a)(5)(A), (a)(5)(B),” both places it appears; and

(B) by striking “and” at the end;

(C) by striking “(a)(5)(C)” and inserting “(a)(5)(A)(iii)”;

(4) by adding at the end the following new paragraphs:

“(4)(A) A fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense punishable under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
“(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection; “(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(ii) or (a)(5)(A)(iii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.”.

(c) DEFINITIONS.—Subsection (e) of section 1090 of title 18, United States Code is amended—

(1) in paragraph (2)(B), by inserting “including a computer located outside the United States” before the semicolon;

(2) in paragraph (7), by striking “and” at the end;

(3) by striking paragraph (8) and inserting the following new paragraph (8):

“(8) the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information;”;

(4) is paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following new paragraphs:

“103(c) the term ‘conviction’ shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, and exceeding authorized access, to a computer;

‘11(1) the term ‘loss’ includes any reasonable cost to any victim, including the cost of respondent to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, and any other consequential damages incurred because of interruption of service;

‘12 the term ‘person’ means an individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity;’.

(d) DAMAGES IN CIVIL ACTIONS.—Subsection (g) of section 1030 of title 18, United States Code is amended—

(1) by striking the second sentence and inserting the following new sentences: “A suit for a violation of subsection (a)(3) may be brought only if conduct involves one of the factors enumerated in subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(A)(i) are limited to economic damages;” and

(2) by adding at the end the following: “No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.”;

(e) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER FRAUD AND ABUSE.—Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to ensure that any individual convicted of a violation of section 1030 of title 18, United States Code, can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.

SEC. 816. ADDITIONAL DEFENSE TO CIVIL ACTIONS INVOLVING NATIONAL SECURITY RECORDS IN RESPONSE TO GOVERNMENT REQUESTS.

Section 2707(e)(1) of title 18, United States Code, is amended by inserting after “or statute” the following: “including a request of a governmental entity under section 2703(f) of this title”.

SEC. 817. DEVELOPMENT AND SUPPORT OF CYBERSECURITY FORENSIC ABILITIES.

(a) In General.—The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability—

(1) to provide examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);

(2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);

(3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;

(4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors through the use of multijurisdictional task forces; and

(5) to carry out such other activities as the Attorney General considers appropriate.

(b) AUTHORIZATION.—There is hereby authorized to be appropriated in each fiscal year $50,000,000 for purposes of carrying out this section.

(c) AVAILABILITY.—Amounts appropriated pursuant to the authorization of appropriated in paragraph (1) shall remain available until expended.

TITLe IX—IMPROVED INTELLIGENCE

SEC. 901. RESPONSIBILITIES OF DIRECTOR OF CENTRAL INTELLIGENCE REGARDING INTELLIGENCE COLLECTED UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 103(c) of the National Security Act of 1947 (50 U.S.C. 403–3(c)) is amended—

(1) by redesigning paragraphs (6) and (7) as paragraphs (7) and (8), respectively; and

(2) by inserting after paragraph (5) the following new paragraph (6):

“(6) established priorities and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and any procedure authorized by the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance operations other than those otherwise authorized by statute or executive order.”;

SEC. 902. INCLUSION OF INTERNATIONAL TERRORIST ACTIVITIES WITHIN SCOPE OF FOREIGN INTELLIGENCE UNDER NATIONAL SECURITY ACT OF 1947.

Section 3 of the National Security Act of 1947 (50 U.S.C. 401a) is amended—

(1) in paragraph (2), by inserting before the period the following: “(A) any international terrorist activities”; and

(2) in paragraph (3), by striking “and activities conducted” and inserting “, and activities conducted”.

SEC. 903. SENSE OF CONGRESS ON THE ESTABLISHMENT AND MAINTENANCE OF INTELLIGENCE RELATIONSHIPS TO ACQUIRE INFORMATION ON TERRORISTS AND TERRORIST ORGANIZATIONS.

It is the sense of Congress that officers and employees of the intelligence community of the Federal Government, acting within the course of their official duties, should be encouraged, and should make every effort, to establish and maintain intelligence relationships with any person or group for the purpose of engaging in lawful intelligence activities, including the acquisition of information on the identity, location, financial status, affiliations, or intentions of a terrorist or terrorist organization, or information on any other person, entity, or group (including a foreign government engaged in harboring, financing, aiding, or assisting a terrorist or terrorist organization.

SEC. 904. TEMPORARY AUTHORITY TO DEFER SUBMITTAL TO CONGRESS OF REPORTS ON INTELLIGENCE-RELATED MATTERS.

(a) AUTHORITY TO DEFER.—The Secretary of Defense, Attorney General, and Director of Central Intelligence each may, during the effective period of this section, defer the date of submittal to Congress of any covered intelligence report under the jurisdiction of such official until February 1, 2002.

(b) COVERED INTELLIGENCE REPORT.—Except as provided in subsection (c), for purposes of subsection (a), a covered intelligence report is as follows: any report on intelligence or intelligence-related activities of the United States Government that is required to be submitted to Congress by an element of the intelligence community during the effective period of this section.

(c) EXCEPTION FOR CERTAIN REPORTS.—For purposes of subsection (a), any report required by section 502 or 503 of the National Security Act of 1947 (50 U.S.C. 413a, 413b) is not a covered intelligence report.

(d) NOTICE TO CONGRESS.—Upon deferring the date of submittal to Congress of a covered intelligence report under the jurisdiction of such official to a date after February 1, 2002, if such official submits to the committees of Congress specified in subsection (b)(2) before February 1, 2002, a certification that preparation and submittal of the covered intelligence report shall submit to Congress notice of the deferral. Notice of deferral of a report on intelligence or intelligence-related activities of the United States Government that is required to be submitted to Congress by an element of the intelligence community that is otherwise authorized by law, if any, under which the report would otherwise be submitted to Congress.

(e) EXTENSION OF DEFERRAL.—(1) Each official specified in subsection (a) may defer the date of submittal to Congress of a covered intelligence report under the jurisdiction of such official to a date after February 1, 2002, if such official submits to the committees of Congress specified in subsection (b)(2) before February 1, 2002, a certification that preparation and submittal of the covered intelligence report shall submit to Congress notice of the deferral. Notice of deferral of a report on intelligence or intelligence-related activities of the United States Government that is otherwise authorized by law, if any, under which the report would otherwise be submitted to Congress.

(f) EFFECTIVE PERIOD.—The effective period of this section is the period beginning on the date of the enactment of this Act and ending on February 1, 2002.

(g) ELEMENT OF THE INTELLIGENCE COMMUNITY DEFINED.—In this section, the term “element of the intelligence community” means any element of the intelligence community specified or under section 3(c) of the National Security Act of 1947 (50 U.S.C. 401a(4)).
SEC. 905. DISCLOSURE TO DIRECTOR OF CENTRAL INTELLIGENCE OF FOREIGN INTELLIGENCE-RELATED INFORMATION WITH RESPECT TO CRIMINAL INVESTIGATIONS.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.) is amended—

(1) by redesignating subsection 105B as section 105C; and

(2) by inserting after section 105A the following new section 105B:—

"SEC. 105B. DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN CRIMINAL INVESTIGATIONS; NOTICE OF CRIMINAL INVESTIGATIONS OF FOREIGN INTELLIGENCE SOURCES.

"(a) PROCEDURES. —(1) Except as otherwise provided by law and subject to paragraph (2), the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of Central Intelligence, pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired by an element of the Department of Justice or an element of such agency, as the case may be, in the course of a criminal investigation.

"(2) The Attorney General by regulation and in consultation with the Director of Central Intelligence, shall identify exceptions to the applicability of paragraph (1) for one or more classes of foreign intelligence, or for foreign intelligence with respect to one or more targets or matters, if the Attorney General determines that disclosure of such foreign intelligence under that paragraph would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests.

"(b) PROCEDURES FOR NOTICE OF CRIMINAL INVESTIGATIONS. —Not later than 180 days after the date of enactment of this Act, the Attorney General, in consultation with the Director of Central Intelligence, shall develop guidelines to ensure that after receipt of a report from an element of the intelligence community of a criminal investigation in which foreign intelligence sources are involved, or that information relating to such activities or sources may warrant investigation as criminal activity, the Attorney General provides notice to the Director of Central Intelligence, within a reasonable period of time to allow him to take action to commence, or decline to commence, a criminal investigation of such activity.

"(c) PROCEDURES.—The Attorney General shall develop for the administration of this section, including the disclosure of foreign intelligence by elements of the Department of Justice, and elements of other departments and agencies of the Federal Government, under subsection (a) and the provision of notice with respect to criminal investigations under subsection (b).

"SEC. 105C. PROTECTION OF THE OPERATIONAL FILES OF THE NATIONAL IMAGERY AND MAPPING AGENCY.

SEC. 906. FOREIGN TERRORIST ASSET TRACKING CENTER.

(a) REPORT ON RECONFIGURATION.—Not later than February 1, 2002, the Attorney General of the Central Intelligence Agency, and the Secretary of the Treasury shall jointly submit to Congress a report on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the Office of Foreign Assets Control of the Department of the Treasury in order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations.

(b) REPORT REQUIREMENTS.—(1) In preparing the report under subsection (a), the Attorney General shall consider whether, and to what extent, the capacities and resources of the Financial Crimes Enforcement Center of the Department of the Treasury may be integrated into the capability contemplated by the report.

(2) If the Attorney General, Secretary, and the Director determine that it is feasible and desirable to undertake the reconfiguration described in subsection (a) in order to establish the capability described in that subsection, the Attorney General, the Secretary, and the Director shall include with the report under that subsection a detailed proposal for legislation to achieve the reconfiguration.

SEC. 907. NATIONAL VIRTUAL TRANSLATION CENTER.

(a) REPORT ON ESTABLISHMENT.—Not later than February 1, 2002, the Director of Central Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the appropriate committees of Congress a report on the establishment and maintenance within the intelligence community of an element for purposes of providing timely and accurate translations of foreign intelligence for all other elements of the intelligence community. In the report, the element shall be referred to as the "National Virtual Translation Center.

(b) REPORT REQUIREMENTS.—The report on the element described in paragraph (1) shall discuss the use of state-of-the-art communications technology, the integration of existing translation capabilities in the intelligence community, and the utilization of remote-connection capacities so as to minimize the need for a central physical facility for the element.

SEC. 908. TRAINING OF GOVERNMENT OFFICIALS REGARDING IDENTIFICATION AND USE OF FOREIGN INTELLIGENCE.

(a) PROGRAM REQUIRED.—The Attorney General shall, in consultation with the Director of Central Intelligence, carry out a program to provide appropriate training to officials described in subsection (b) in order to assist such officials in identifying foreign intelligence information in the course of their duties; and

(b) OFFICIALS.—The officials provided training under subsection (a) are, at the discretion of the Attorney General and the Director, the following:

(1) Officials of the Federal Government who are not ordinarily engaged in the collection, dissemination, and use of foreign intelligence in the performance of their duties.

(2) Officials of State and local governments with a counterterrorism mission, or may encounter in the course of a terrorist event, foreign intelligence in the performance of their duties.

(c) AUTHORIZATION OF APPROPRIATIONS.—The fiscal year 2002 amounts authorized to be appropriated for the Department of Justice such sums as may be necessary for purposes of carrying out the program required by subsection (a)

Mr. REID. Mr. President, I move to reconsider the vote.

I move to lay that motion on the table.

The motion to lay on the table was agreed to.

MORNING BUSINESS

Mr. REID. Mr. President, I ask unanimous consent that the Senate go into a period of morning business with Senators permitted to speak therein for a period not to exceed 10 minutes.

Mr. KYL. I object.

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

The PENTAGON MEMORIAL SERVICE

Mr. MCCAII. Mr. President, on this solemn day, one month since the horrific terrorist attacks on American citizens, our institutions, and our way of life, memorial services were held today in New York City and Arlington, VA. President Bush, whom I commend for his leadership and strong efforts to unify our Nation at this difficult time in our history, spoke today at the Pentagon commemoration honoring the victims of these attacks. His remarks were eloquent and very moving to the families and members of our armed forces who attended the service. I was asked to submit the President's remarks for the Record, and I am privileged to do so.

I have also included the remarks of the Secretary of Defense, the Honorable Donald H. Rumsfeld, and the