Ron Olson, South Dakota Corn Growers Association.
Darrell Cruea, South Dakota Department of Agriculture.
Nettie Myers, South Dakota Department of Environment and Natural Resources.
John Cooper, South Dakota Department of Game, Fish, and Parks.
Michael Held, South Dakota Farm Bureau.
Dennis Wiese, South Dakota Farmers Union.
Ron Ogren, South Dakota Grassland Coalition.
Don Marquart, South Dakota Lakes and Streams Association, Inc.
Mari Beth Baumberger, South Dakota Pork Producers Council.
Lawrence Novotny, South Dakota Resources Coalition.
Delbert Tschakert, South Dakota Soybean Association.
Bart Blum, South Dakota Stockgrowers.
Rick Vallery, South Dakota Wheat, Inc.
Chris Hesla, South Dakota Wildlife Federation.
Ron Schauer, Wildlife Society, South Dakota Chapter.
Dennis Johnson, Turner County Conservation District.
Carl Madsen, U.S. Fish and Wildlife Service.
Amond Hanson, Vermillion Basin Water Development District.
Lester Austin, Vermillion River Watershed Authority.
David Hauschild, Central Planes Water Development District and South Dakota Water Congress.

Mr. JOHNSON. Mr. President, given that over thirty groups and several more individuals were active participants in this historic agreement in South Dakota—it is impossible to aptly recognize every single one that deserves credit for this achievement. However, I cannot overlook the efforts of two real champions of this agreement and pilot project—two individuals who worked closely with me to make sure their idea developed from a South Dakota agreement to a six-state pilot project that the 106th Congress enacted and that the President will sign into law.

Paul Shubeck, a Centerville, South Dakota farmer and Carl Madsen, a Brookings, South Dakota private lands coordinator for the Fish and Wildlife Service developed this plan and helped negotiate its path through Congress.

Paul Shubeck greatly impressed me with his ability to shepherd this proposal, not only within a diverse coalition of South Dakota groups who normally do not tend to agree on wetlands matters, but also at the national level where he consistently advocated on behalf of the American family farmer who just wants a chance to produce a crop on his land and protect the environment all at the same time. Paul's drive and ability to compromise were key to the success of our pilot project.

Carl Madsen was a real source of passion for this project and provided us with a sense for the big picture—how our pilot would and could work in South Dakota and other parts of the United States. Carl's deep knowledge of wetlands and conservation policy provided us with critical technical assistance to ensure this pilot project was a credible, practical program.

Many, many more individuals and groups in South Dakota and the United States provided direct assistance to this effort Mr. President, and I want them all to know I am deeply grateful.

Earlier this year Mr. President, Senator DASCHLE and I urged Secretary Dan Glickman and the United States Department of Agriculture (USDA) to implement the South Dakota agreement in principle on an administrative basis. While USDA was supportive of the concept, they were reluctant to implement such a program without a clearer understanding of the purpose and implications of the program.

In response, on July 7, I brought a top USDA official to a farm near Renner, South Dakota where we met with several groups and individuals to discuss how to conserve these critical wetlands yet compensate farmers for taking the wetlands out of crop production. It was there that some suggested a pilot project would be the best route to take. Then, on July 27, Senator DASCHLE and I introduced S. 2980 to create a South Dakota pilot project permitting up to 150,000 acres of farmable wetlands into CRP.

Once S. 2980 was introduced, national conservation, wildlife, and farm organizations took interest and requested that we expand the pilot to cover more than South Dakota. The proposal adopted by Congress is the result of weeks of negotiations between Senator DASCHLE, myself, USDA, Senator LUGAR who serves as the Chairman of the Senate Agriculture Committee, and several national groups who now support the pilot. The changes resulted in expanding this program to the Prairie Pothole Region of the United States, including South Dakota, North Dakota, Minnesota, Nebraska, Iowa, and Montana. It is limited to 500,000 acres in those states, with an assurance that access be distributed fairly among interested CRP participants.

I truly believe this pilot project will provide landowners an alternative to farming these highly sensitive wetlands in order to achieve a number of benefits including; improved water quality, reduced soil erosion, enhanced wildlife habitat, preserved biodiversity, flood control, less wetland drainage, economic compensation for landowners for protecting the sensitive wetlands, and diminished divisiveness over wetlands issues.

Moreover, the pilot project is consistent with the purpose of CRP, and, if successful, could serve as a model for future farm policy as we look toward the next farm bill. I believe Congress will be unable to develop a future farm bill without the support of those in the conservation and wildlife community. I am a strong supporter of conservation programs that protect sensitive soil and water resources, promote wildlife habitat, and provide farmers and landowners with benefits and incentives to conserve land. I have introduced the Flex Fallow Farm Bill Amendment to achieve some of these objectives. It is my hope that the success on our pilot project can serve as a model to once again bring conservation groups together with farm interests in order to develop a well-balanced approach to future farm policy that protects our resources while promoting family-farm agriculture.

Finally, I fully understand the successful adoption of this wetlands pilot project—no matter how important—will not put an end to the ongoing debate over the management of wetlands on farmland. Yet, I really hope that everyone engaged in the debate considers how effective we can be when we cooperate and compromise on this important issue.

PASSAGE OF CERTAIN LEGISLATION

Mr. LEAHY. Mr. President, today we consider four bipartisan bills offered together as a package: the Public Safety Officer Medal of Valor Act, H.R. 46, the Computer Crime Enforcement Act, which I introduced as S. 1314, on July 1, 1999, with Senator DEWINE and is now also co-sponsored by Senators ROBB, HATCH and ABRAHAM; a Hatch-Leahy-Schumer ''Internet Security Act'' amendment; and a Bayh-Grams-Leahy-Cleland ''Protecting Seniors from Fraud Act'' amendment. I thank my colleagues for their hard work on these pieces of legislation, each of which I will discuss in turn.

I support the Public Safety Officer Medal of Valor. I cosponsored the Stevens bill, S. 39, to establish a Public Safety Medal of Valor Act. In April and May, 1999, I made sure that the Senate acted on Senator STEVENS' bill, S. 39.

On April 22, 1999, the Senate Judiciary Committee took up that measure in regular order and reported it unanimously. At that time I congratulated Senator STEVENS and thanked him for his leadership. I noted that we had worked together on a number of law enforcement matters and that the senior Senator from Alaska is a stalwart supporter of the men and women who put themselves at risk to protect us all. I said that I looked forward to enactment of this measure and to seeing the extraordinary heroism of our police, firefighters and correctional officers recognized with the Medal of Valor.

In May, 1999, I was privileged to be on the floor of the Senate when we proceeded to consider S. 39 and passed it unanimously. I took that occasion to commend Senator STEVENS and all who had worked so hard to move this measure in a timely way. That was over one year ago, during National Police Week last year. The measure was sent to the House where it lay dormant for over the rest of last year and most of this one.

The President of the United States came to Capitol Hill to speak at the Law Enforcement Officers Memorial Service on May 15, 2000, and said on that occasion that if Congress would

not act on the Medal of Valor, he was instructing the Attorney General to explore ways to award such recognition by Executive action.

Unfortunately, these calls for action did not waken the House from its slumber on this matter and the House of Representatives refused to pass the Senate-passed Medal of Valor bill. Instead, over the past year, the House has insisted that the Senate take up, fix and pass the House-passed version of this measure if it is to become law. House members have indicated that they are now prepared to accept the Senate-passed text, but insist that it be enacted under the House bill number. In order to get this important measure to the President, that is what we are doing today. We are discharging the House-passed version of that bill, H.R. 46, from the Judiciary Committee, adopting a complete substitute to bring it into conformance with the Stevens bill, S. 39, and sending it back to the House.

Senator STEVENS' version of this bill which I cosponsored is preferable to the House-passed bill, H.R. 46, and I am pleased that the version we pass today conforms to the Senate version.

For example, the House-passed version would limit the number of possible recipients of the Medal of Valor to 5 in any given year. The Stevens bill had allowed for up to 10 in any year. There is no requirement that the Board select the maximum possible recipients in any year, but I fear that 5 may be an artificially low ceiling for extraordinary valor across this country. I would not want officers from rural areas to be slighted because of such a low number. I would not want firefighters or correctional officers to be slighted. In addition, I can imagine a year where an incident involves a group of officers, maybe even a group numbering more than 5, and recognition of those involved in a single incident could consume all 5 of the awards allowed by the substitute that year and leave others, even others from that incident, without recognition. I believe that the Senate had it right the first time and is getting it right in the version we pass today.

In addition, the House-passed version omits any reference to a role for the Board in the creation of criteria and procedures for recommendations of nominees. The Senate-passed bill would have required the concurrence of the Board in the National Medal of Valor Office's establishing of those criteria. Again, I believe the Senate had it right and that is the version we pass today.

I hope that the proponents of proceeding in this manner and of making these changes in the language of the bill will explain to the Senate and the American people why we have had to wait over a year for action, why the Senate is being asked to act a second time on a bill strikingly similar to S. 39 but under a House number, and why each of these changes are necessary. I wish the House would have just passed S. 39.

The information age is filled with unlimited potential for good, but it also creates a variety of new challenges for law enforcement. A recent survey by the FBI and the Computer Security Institute found that 62 percent of information security professionals reported computer security breaches in the past year. These breaches in computer security resulted in financial losses of more than $120 million from fraud, theft of information, sabotage, computer viruses, and stolen laptops. Computer crime has become a multi-billion dollar problem.

Many of us have worked on these issues for years. In 1984, we passed the Computer Fraud and Abuse Act to criminalize conduct when carried out by means of unauthorized access to a computer. In 1986, we passed the Electronic Communications Privacy Act, ECPA, which I was proud to sponsor, to criminalize tampering with electronic mail systems and remote data processing systems and to protect the privacy of computer users. In 1994, the Violent Crime Control and Law Enforcement Act included the Computer Abuse Amendments which I authored to make illegal the intentional transmission of computer viruses.

In the 104th Congress, Senators KYL, GRASSLEY and I worked together to enact the National Information Infrastructure Protection Act to increase protection under federal criminal law for both government and private computers, and to address an emerging problem of computer-age blackmail in which a criminal threatens to harm or shut down a computer system unless their extortion demands are met. In the 105th Congress, Senators KYL and I also worked together on criminal copyright amendments that became law to enhance the protection of copyrighted works online.

The Congress must be constantly vigilant to keep the law up-to-date with technology. The Computer Crime Enforcement Act, S. 1314, and the Hatch-Leahy-Schumer ''Internet Security Act'' amendment are part of that ongoing effort. These complementary pieces of legislation reflect twin-track progress against computer crime: More tools at the federal level and more resources for local computer crime enforcement. The fact that this is a bipartisan effort is good for technology policy.

But make no mistake about it: even with passage of this legislation, there is more work to be done—both to assist law enforcement and to safeguard the privacy and other important constitutional rights of our citizens. I wish that the Congress had also tackled online privacy in this session, but that will now be punted into the next congressional session.

The legislation before us today does not attempt to resolve every issue. For example, both the Senate and the House held hearings this session about the FBI's Carnivore program. Carnivore is a computer program designed to advance criminal investigations by capturing information in Internet communications pursuant to court orders. Those hearings sparked a good debate about whether advances in technology, like Carnivore, require Congress to pass new legislation to assure that our private Internet communications are protected from government over-reaching while protecting the government's right to investigate crime. I look forward to our discussion of these privacy issues in the next Congress.

The Computer Crime Enforcement Act is intended to help states and local agencies in fighting computer crime. All 50 states have now enacted tough computer crime control laws. They establish a firm groundwork for electronic commerce, an increasingly important sector of the nation's economy.

Unfortunately, too many state and local law enforcement agencies are struggling to afford the high cost of enforcing their state computer crime statutes.

Earlier this year, I released a survey on computer crime in Vermont. My office surveyed 54 law enforcement agencies in Vermont—43 police departments and 11 State's attorney offices—on their experience investigating and prosecuting computer crimes. The survey found that more than half of these Vermont law enforcement agencies encounter computer crime, with many police departments and state's attorney offices handling 2 to 5 computer crimes per month.

Despite this documented need, far too many law enforcement agencies in Vermont cannot afford the cost of policing against computer crimes. Indeed, my survey found that 98 percent of the responding Vermont law enforcement agencies do not have funds dedicated for use in computer crime enforcement. My survey also found that few law enforcement officers in Vermont are properly trained in investigating computer crimes and analyzing cyber-evidence.

According to my survey, 83 percent of responding law enforcement agencies in Vermont do not employ officers properly trained in computer crime investigative techniques. Moreover, my survey found that 52 percent of the law enforcement agencies that handle one or more computer crimes per month cited their lack of training as a problem encountered during investigations. Without the necessary education, training and technical support, our law enforcement officers are and will continue to be hamstrung in their efforts to crack down on computer crimes.

I crafted the Computer Crime Enforcement Act, S. 1314, to address this problem. The bill would authorize a $25 million Department of Justice grant program to help states prevent and prosecute computer crime. Grants under our bipartisan bill may be used to provide education, training, and enforcement programs for local law enforcement officers and prosecutors in

the rapidly growing field of computer criminal justice. Our legislation has been endorsed by the Information Technology Association of America and the Fraternal Order of Police. This is an important bipartisan effort to provide our state and local partners in crime-fighting with the resources they need to address computer crime.

The Internet Security Act of 2000 makes progress to ensure that we are properly dealing with the increase in computer crime. I thank and commend Senators HATCH and SCHUMER for working with me and other Members of the Judiciary Committee to address some of the serious concerns we had with the first iteration of their bill, S. 2448, as it was originally introduced.

Specifically, as introduced, S. 2448 would have over-federalized minor computer abuses. Currently, federal jurisdiction exists for a variety of computer crimes if, and only if, such criminal offenses result in at least $5,000 of damage or cause another specified injury, including the impairment of medical treatment, physical injury to a person or a threat to public safety. S. 2448, as introduced, would have eliminated the $5,000 jurisdictional threshold and thereby criminalized a variety of minor computer abuses, regardless of whether any significant harm resulted.

For example, if an overly-curious college sophomore checks a professor's unattended computer to see what grade he is going to get and accidently deletes a file or a message, current Federal law does not make that conduct a crime. That conduct may be cause for discipline at the college, but not for the FBI to swoop in and investigate. Yet, under the original S. 2448, as introduced, this unauthorized access to the professor's computer would have constituted a federal crime.

Another example is that of a teenage hacker, who plays a trick on a friend by modifying the friend's vanity Web page. Under current law, no federal crime has occurred. Yet, under the original S. 2448, as introduced, this conduct would have constituted a federal crime.

As America Online correctly noted in a June, 2000 letter, ''eliminating the $5,000 threshold for both criminal and civil violations would risk criminalizing a wide range of essentially benign conduct and engendering needless litigation. . . .'' Similarly, the Internet Alliance commented in a June, 2000 letter that ''[c]omplete abolition of the limit will lead to needless federal prosecution of often trivial offenses that can be reached under state law. . . .''

Those provisions were overkill. Our federal laws do not need to reach each and every minor, inadvertent and harmless computer abuse—after all, each of the 50 states has its own computer crime laws. Rather, our federal laws need to reach those offenses for which federal jurisdiction is appropriate.

Prior Congresses have declined to over-federalize computer offenses as proposed in S. 2448, as introduced, and sensibly determined that not all computer abuses warrant federal criminal sanctions. When the computer crime law was first enacted in 1984, the House Judiciary Committee reporting the bill stated:

> the Federal jurisdictional threshold is that there must be $5,000 worth of benefit to the defendant or loss to another in order to concentrate Federal resources on the more substantial computer offenses that affect interstate or foreign commerce. (H. Rep. 98–894, at p. 22, July 24, 1984).

Similarly, the Senate Judiciary Committee under the chairmanship of Senator THURMOND, rejected suggestions in 1986 that ''the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered.'' (S. Rep. 99–432, at p. 4, September 3, 1986).

The Hatch-Leahy-Schumer substitute amendment to S. 2448, which was reported unanimously by the Judiciary Committee on October 5th, addresses those federalism concerns by retaining the $5,000 jurisdictional threshold in current law. That Committee-reported substitute amendment, with the additional refinements reflected in the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46, which the Senate considers today, makes other improvements to the original bill and current law, as summarized below.

First, titles II, III, IV and V of the original bill, S. 2448, about which various problems had been raised, are eliminated. For example, title V of the original bill would have authorized the Justice Department to enter into Mutual Legal Assistance Treaties (MLAT) with foreign governments that would allow the Attorney General broad discretion to investigate lawful conduct in the U.S. at the request of foreign governments without regard to whether the conduct investigated violates any Federal computer crime law. In my view, that discretion was too broad and troubling.

Second, the amendment includes an authorization of appropriations of $5 million to the Computer Crime and Intellectual Property (CCIP) section within the Justice Department's Criminal Division and requires the Attorney General to make the head of CCIP a ''Deputy Assistant Attorney General,'' which is not a Senate-confirmed position, in order to highlight the increasing importance and profile of this position. This authorized funding level is consistent with an amendment I sponsored and circulated to Members of the Judiciary Committee to improve S. 2448 and am pleased to see it incorporated into the Internet Security Act amendment to H.R. 46.

Third, the amendment modifies section 1030 of title 18, United States Code, in several important ways, including providing for increased and enhanced penalties for serious violations of federal computer crime laws, clarifying the definitions of ''loss'' to ensure that the full costs to a hacking victim are taken into account and of ''protected computer'' to facilitate investigations of international computer crimes affecting the United States, and preserving the existing $5,000 threshold and other jurisdictional prerequisites for violations of section 1030(a)(5)—i.e., no Federal crime has occurred unless the conduct (1) causes loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value, (2) impairs the medical care of another person, (3) causes physical injury to another person, (4) threatens public health or safety, or (5) causes damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

The amendment clarifies the precise elements of the offense the government must prove in order to establish a violation by moving these prerequisites from the current definition of ''damage'' to the description of the offense. In addition, the amendment creates a new category of felony violations where a hacker causes damage to a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Currently, the Computer Fraud and Abuse Act provides for federal criminal penalties for those who intentionally access a protected computer or cause an unauthorized transmission to a protected computer and cause damage. ''Protected computer'' is defined to include those that are ''used in interstate or foreign commerce.'' See 18 U.S.C. 1030(e)(2)(B). The amendment would clarify the definition of ''protected computer'' to ensure that computers which are used in interstate or foreign commerce but are located outside of the United States are included within the definition of ''protected computer'' when those computers are used in a manner that affects interstate or foreign commerce or communication of this country. This will ensure that our government will be able to conduct domestic investigations and prosecutions against hackers from this country who hack into foreign computer systems and against those hacking through the United States to other foreign venues. Moreover, by clarifying the fact that a domestic offense exists, the United States will be able to use speedier domestic procedures in support of international hacker cases, and create the option of prosecuting such criminals in the United States.

The amendment also adds a definition of ''loss'' to the Computer Fraud and Abuse Act. Current law defines the term ''damage'' to include impairment of the integrity or availability of data, programs, systems or information causing a ''loss aggregating at least $5,000 in value during any 1-year period to one or more individuals.'' See 18 U.S.C. § 1030(e)(8)(A). The new definition of ''loss'' to be added as section 1030(e)(11) will ensure that the full

costs to victims of responding to hacking offenses, conducting damage assessments, restoring systems and data to the condition they were in before an attack, as well as lost revenue and costs incurred because of an interruption in service, are all counted. This statutory definition is consistent with the definition of ''loss'' appended by the U.S. Sentencing Commission to the Federal Sentencing Guidelines (see U.S.S.G. §2B1.1 Commentary, Application note 2), and will help reconcile procedures by which prosecutors value loss for charging purposes and by which judges value loss for sentencing purposes. Getting this type of true accounting of ''loss'' is important because loss amounts can be used to calculate restitution and to determine the appropriate sentence for the perpetrator under the sentencing guidelines.

Fourth, subsection 3(e) of the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46 clarifies the grounds for obtaining damages in civil actions for violations of the Computer Fraud and Abuse Act. Current law authorizes a person who suffers ''damage or loss'' from a violation of section 1030 to sue the violator for compensatory damages or injunctive or other equitable relief, and limits the remedy to ''economic damages'' for violations ''involving damage as defined in subsection (e)(8)(A),'' relating to violations of 1030(a)(5) that cause loss aggregating at least $5,000 during any 1-year period. To take account of both the new definition of ''loss'' and the incorporation of this jurisdictional threshold into the description of the offense (rather than the current definition of ''damage''), the amendment strikes the reference to subsection (e)(8)(A) in the current civil action provision and retains Congress' previous intent to allow civil plaintiffs only economic damages for violations of section 1030(a)(5) that do not also affect medical treatment, cause physical injury, threaten public health and safety or affect computer systems used in furtherance of the administration of justice, the national defense or national security.

The Congress provided this civil remedy in the 1994 amendments to the Act, which I originally sponsored with Senator Gordon Humphrey, to enhance privacy protection for computer communications and the information stored on computers by encouraging institutions to improve computer security practices, deterring unauthorized persons from trespassing on computer systems of others, and supplementing the resources of law enforcement in combating computer crime. [See The Computer Abuse Amendments Act of 1990: Hearing Before the Subcomm. On Technology and the Law of the Senate Comm. On the Judiciary, 101st Cong., 2nd Sess., S. Hrg. 101–1276, at pp. 69, 88, 92 (1990); see also Statement of Senator Humphrey, 136 Cong. Rec. S18235 (1990) (''Given the Government's limited capacity to pursue all computer crime cases, the existence of this limited civil remedy will serve to enhance deterrence in this critical area.'')]. The ''new, civil remedy for those harmed by violations of the Computer Fraud and Abuse Act'' was intended to ''boost the deterrence of the statute by allowing aggrieved individuals to obtain relief.'' [S. Rep. No. 101–544, 101st Cong., 2d Sess., p. 6–7 (1990); see also Statement of Senator LEAHY, 136 Cong. Rec. S18234 (1990)]. We certainly and expressly did not want to ''open the floodgates to frivolous litigation.'' [Statement of Senator LEAHY, 136 Cong. Rec. S4614 (1990)].

At the time the civil remedy provision was added to the Computer Fraud and Abuse Act, this Act contained no prohibition against negligently causing damage to a computer through unauthorized access, reflected in current law, 18 U.S.C. §1030(a)(5)(C). That prohibition was added only with subsequent amendments made in 1996, as part of the National Information Infrastructure Protection Act. Nevertheless, the civil remedy has been interpreted in some cases to apply to the negligent manufacture of computer hardware or software. Most notably See, e.g., Shaw v. Toshiba America Information Systems, Inc., NEC, 91 F. Supp. 2d 926 (E.D. TX 1999) (court interpreted the term transmission to include sale of computers with a minor design defect).

The Hatch-Leahy-Schumer Internet Security Act amendment adds a new sentence clarifying that civil actions may not be brought ''for the negligent design or manufacture of computer hardware, computer software, or firmware.'' This change should ensure that the civil remedy is a robust option for private enforcement actions, while limiting its applicability to cases that are more appropriately governed by contractual warranties, state tort law and consumer protection laws.

Fifth, sections 104 and 109 of the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46 authorize criminal and civil forfeiture of computers, equipment, and other personal property used to violate the Computer Fraud and Abuse Act, as well as real and personal property derived from the proceeds of computer crime. Property, both real and personal, which is derived from proceeds traceable to a violation of section 1030, is currently subject to both criminal and civil forfeiture. See 18 U.S.C. §981(a)(1)(C) and 982(a)(2)(B). Thus, the amendment would clarify in section 1030 itself that forfeiture applies and extend the application of forfeiture to property that is used or intended to be used to commit or to facilitate the commission of a computer crime. In addition, to deter and prevent piracy, theft and counterfeiting of intellectual property, the section 109 of the amendment allows forfeiture of devices, such as replicators or other devices used to copy or produce computer programs to which counterfeit labels have been affixed.

The forfeiture amendments are based on the procedures set forth in section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. §853) and chapter 46 of title 18, as revised this year by the Civil Asset Forfeiture Reform Act of 2000, and thereby build in all of the existing due process protections in existing law.

In particular, these provisions protect innocent property owners. Sections 104 and 109 subject to forfeiture only property which belongs to the person who knowingly violated the law, not innocent third parties whose property unbeknownst to them was used to violate the law. Under existing law, for example, a drug trafficker may avail herself of the facilities of a telephone company to communicate with her source of narcotics, send pager messages to drug confederates and signal the buyer by beeper when the sale is ready to be consummated, but the law does not authorize forfeiture of the facilities of the telephone company which was neither aware of nor intended the drug deal. Likewise, a rogue employee of an Internet access provider or other computer hacker or cyber-criminal will almost necessarily use the facilities of an Internet access provider to commit her violation, but Sections 104 and 109 do not authorize forfeiture of the provider's facilities simply because its facilities were used.

The criminal forfeiture provision in section 104 specifically states that only the ''interest of such person,'' referring to the defendant who committed the computer crime, is subject to forfeiture. Moreover, the criminal forfeiture authorized by Sections 104 and 109 is made expressly subject to Section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970, but subsection (d) of section 413 is expressly exempted from application to Section 104 and 109. That subsection (d) creates a rebuttable presumption of forfeiture in favor of the government where a person convicted of a felony acquired the property during the period that the crime was committed or within a reasonable time after such period and there was no likely source for such property other than the criminal violation. Thus, by making subsection (d) inapplicable, Sections 104 and 109 make it more difficult for the government to prove that the property should be forfeited.

Chapter 46 of title 18, to which the civil forfeiture provision of section 104 is expressly made subject, provides property owners with important safeguards from unwarranted forfeitures and government overreaching. First, the civil forfeiture law states that ''[n]o property shall be forfeited . . . to the extent of the interest of an owner or lien holder by reason of any act or omission . . . to have been committed without the knowledge of that owner or lien holder.'' 18 U.S.C. § 981(a)(2).

Furthermore, the chapter puts the burden on the government to prove forfeiture by a preponderance of the evidence, permits courts to appoint counsel to represent indigent owners where the owner is represented by a court-appointed attorney in a related federal criminal case, and permits recovery of attorney fees and costs for property owners not appointed counsel if they substantially prevail on their claim.

Sixth, the amendment contains certain provisions intended to deter computer crimes by juveniles. The amendment would permit federal prosecution, under 18 U.S.C. § 5032, of juveniles as juveniles upon certification by the Attorney General, after investigation, that the offense charged is one of the most serious felonious violations of our federal computer crime laws and that there is a substantial Federal interest in the case or the offense to warrant the exercise of Federal jurisdiction. The computer crime offenses that would qualify for federal prosecution of a juvenile offender as a juvenile are: violations of 1030(a)(1) (accessing a computer and obtaining information relating to national security with reason to believe the information could be used to the injury of the United States or to the advantage of a foreign nation and willfully retaining or transmitting that information or attempting to do so); (a)(2)(B) (intentionally accessing without authorization a federal government computer and obtaining information); (a)(3) (intentionally accessing without authorization a federal government computer and affecting the use by or for the government); and (a)(5)(A)(i) (knowingly causing the transmission of a program to intentionally cause damage without authorization to a protected computer).

The amendment would also authorize a judge to exercise discretion and impose as part of a sentence for a violation of the Computer Fraud and Abuse Act termination of or ineligibility for federal financial assistance for education at a post-secondary institution. The court is expressly authorized to reinstate such eligibility upon motion of the defendant.

Unlike the version reported by the Judiciary Committee, the amendment does not require that prior delinquency adjudications of juveniles for violations of the Computer Fraud and Abuse Act be counted under the definition of ''conviction'' for purposes of enhanced penalties. This is an improvement that I urged since juvenile adjudications simply are not criminal convictions. Juvenile proceedings are more informal than adult prosecutions and are not subject to the same due process protections. Consequently, counting juvenile adjudications as a prior conviction for purposes of the recidivist sanctions under the amendment would be unduly harsh and unfair. In any event, prior juvenile delinquency adjudications are already subject to sentencing enhancements under certain circumstances under the Sentencing Guidelines. See, e.g., U.S.S.G. § 411.2(d) (upward adjustments in sentences required for each juvenile sentence to confinement of at least sixty days and for each juvenile sentence imposed within five years of the defendant's commencement of instant offense).

Seventh, section 108 of the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46 would authorize the interception of wire and oral communications relating to computer fraud and abuse violations by expanding the enumerated list of predicate offenses that may support such authority to include felony violations of section 1030. Under current law, federal investigators and prosecutors have the authority to obtain an order for interception of electronic communications, such as e-mail, when investigating any felony, including a felony violation of Section 1030. Current law, however, does not permit federal investigators and prosecutors to intercept wire or oral communications in investigations of such crimes.

Section 108 addresses this anomaly by adding felony violations of Section 1030 to the list of federal crimes for which federal law enforcement officials may seek evidence by intercepting wire or oral communications. Applications for such interception are to be governed by the same stringent Title III requirements that govern all such applications. See 18 U.S.C. § 2510 et seq.

Some have objected to this provision, questioning the necessity of adding computer crimes to the list of crimes for which interception of wire and oral communications are authorized since this provision would, for example, permit government wiretapping for some relatively minor computer felonies. I disagree. We have come to rely on computers for everything from banking and stock-trading to travel reservations to our most intimate personal conversations with friends and family. Opportunists are exploiting our reliance on computers to advance fraudulent schemes or just for the sport of disruption. We have seen the global havoc that is threatened by a lone hacker transmitting a single virus. Giving law enforcement a full complement of tools to fight computer crime serves to protect the security, confidentiality and privacy of our computer communications and stored electronic information. That there are some computer felonies that are less serious than other computer felonies that might not be as worthy of a wiretap is true of all felonies. The stringent procedural requirements for wiretaps and the investment in time and resources necessary to execute a wiretap within the bounds of the law provide incentive for law enforcement to make prudent use of this important investigative tool in computer fraud and abuse cases.

Developments in technology have placed wire, oral and electronic communications on more equal footing in terms of frequency of use, expectation of privacy, and exploitation for criminal purposes. The law should recognize that more equal footing, particularly for electronic messages, and accord the same privacy safeguards to electronic communications as apply to both oral and wire communications. In fact, the Administration has proposed such changes in the legislation transmitted to the Congress in July, 2000 called the ''Enhancement of Privacy and Public Safety in Cyberspace Act.'' For example, the Administration's proposal would apply existing prerequisites for court-authorized wire communications, such as high-level official approval and investigation of an enumerated predicate offense (rather than any felony), to most electronic communications, such as e-mails and fax transmissions. Unfortunately, as I have noted, we have been unable to reach a consensus on privacy legislation in general or on this more specific instance where additional legislative attention is needed. These are matters that should be addressed.

Eighth, the amendment changes a current directive to the Sentencing Commission enacted as section 805 of the Antiterrorism and Effective Death Penalty Act of 1996, P.L. 104–132, that imposed a 6-month mandatory minimum sentence for any conviction of the sections 1030(a)(4) or (a)(5) of title 18, United States code. The Administration has noted that ''[i]n some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under the statute, knowing that the result would be mandatory imprisonment.'' Clearly, mandatory imprisonment is not always the most appropriate remedy for a federal criminal violation, and the ironic result of this ''get tough'' proposal has been to discourage prosecutions that might otherwise have gone forward. The amendment eliminates that mandatory minimum term of incarceration for misdemeanor and less serious felony computer crimes.

Ninth, section 110 of the amendment directs the Sentencing Commission to review and, where appropriate, adjust sentencing guidelines for computer crimes to address a variety of factors, including to ensure that the guidelines provide sufficiently stringent penalties to deter and punish persons who intentionally use encryption in connection with the commission or concealment of criminal acts.

The Sentencing Guidelines already provide for enhanced penalties when persons obstruct or impede the administration of justice, see U.S.S.G. §3C1.1, or engage in more than minimal planning, see U.S.S.G. §2B1.1(b)(4)(A). As the use of encryption technology becomes more widespread, additional guidance from the Sentencing Commission would be helpful to determine the circumstances when such encryption use would warrant a guideline adjustment. For example, if a defendant employs an encryption product that

works automatically and transparently with a telecommunications service or software product, an enhancement for use of encryption may be not be appropriate, while the deliberate use of encryption as part of a sophisticated and intricate scheme to conceal criminal activity and make the offense, or its extent, difficult to detect, may warrant a guideline enhancement either under existing guidelines or a new guideline.

Tenth, section 105 of the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46 would eliminate certain statutory restrictions on the authority of the United States Secret Service (''Secret Service''). Under current law, the Secret Service is authorized to investigate offenses under six designated subsections of 18 U.S.C. §1030, subject to agreement between the Secretary of the Treasury and the Attorney General: subsections (a)(2)(A) (illegally accessing a computer and obtaining financial information); (a)(2)(B) (illegally accessing a computer and obtaining information from a department or agency of the United States); (a)(3) (illegally accessing a non-public computer of a department or agency of the United States either exclusively used by the United States or used by the United States and the conduct affects that use by or for the United States); (a)(4) (accessing a protected computer with intent to defraud and thereby furthering the fraud and obtaining a thing of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in a one-year period); (a)(5) (knowingly causing the transmission of a program, information, code or command and thereby intentionally and without authorization causing damage to a protected computer; and illegally accessing a protected computer and causing damage recklessly or otherwise); and (a)(6) (trafficking in a password with intent to defraud).

The Secret Service is not authorized to investigate offenses under subsection (a)(1) (accessing a computer and obtaining information relating to national security with reason to believe the information could be used to the injury of the United States or to the advantage of a foreign nation and willfully retaining or transmitting that information or attempting to do so); (a)(2)(C) (illegally accessing a protected computer and obtaining information where the conduct involves an interstate or foreign communication); and (a)(7) (transmitting a threat to damage a protected computer with intent to extort).

Section 105 of the Internet Security Act removes these limitations on the authority of the Secret Service and authorizes the Secret Service to investigate any offense under Section 1030 subject to agreement between the Secretary of the Treasury and the Attorney General. Section 105 also makes a stylistic change, describing the interagency agreement as ''between'' the Secretary of the Treasury and the Attorney General rather than one ''which shall be entered into by'' them.

Prior to 1996 amendments to the Computer Fraud and Abuse Act, the Secret Service was authorized to investigate all violations of Section 1030. According to the 1996 Committee Reports of the 104th Congress, 2nd Session, the 1996 amendments attempted to concentrate the Secret Service' s jurisdiction on certain subsections considered to be within the Secret Service's traditional jurisdiction and not grant authority in matters with a national security nexus. According to the Administration, which first proposed the elimination of these statutory restrictions in connection with transmittal of its comprehensive crime bill, the ''21st Century Law Enforcement and Public Safety Act,'' however, these specific enumerations of investigative authority ''have the potential to complicate investigations and impede interagency cooperation.'' (See Section-by-section Analysis, SEC. 3082, for ''21st Century Law Enforcement and Public Safety Act'').

The current restrictions, for example, risk hindering the Secret Service from investigating ''hacking'' into White House computers or investigating threats against the President that may be delivered by such a ''hacker,'' and fulfilling its mission to protect financial institutions and the nation's financial infrastructure. The provision thus modifies existing law to restore the Secret Service's authority to investigate violations of Section 1030, leaving it to the Departments of Treasury and Justice to determine between them how to allocate workload and particular cases.

Eleventh, section 107 of the Hatch-Leahy-Schumer Internet Security Act amendment would provide an additional defense to civil actions relating to preserving records in response to government requests. Current law authorizes civil actions and criminal liability for unauthorized interference with or disclosures of electronically stored wire or electronic communications under certain circumstances. 18 U.S.C. §§ 2701, et seq. A provision of that statutory scheme makes clear that it is a complete defense to civil and criminal liability if the person or entity interfering with or attempting to disclose a communication does so in good faith reliance on a court warrant or order, grand jury subpoena, legislative or statutory authorization. 18 U.S.C. § 2707(e)(1).

Current law, however, does not address one scenario under which a person or entity might also have a complete defense. A provision of the same statutory scheme currently requires providers of wire or electronic communication services and remote computing services, upon request of a governmental entity, to take all necessary steps to preserve records and other evidence in its possession for a renewal period of 90 days pending the issuance of a court order or other process requiring disclosure of the records or other evidence. 18 U.S.C. § 2703(f). Section 2707(e)(1), which describes the circumstances under which a person or entity would have a complete defense to civil or criminal liability, fails to identify good faith reliance on a governmental request pursuant to Section 2703(f) as another basis for a complete defense. Section 107 modifies current law by addressing this omission and expressly providing that a person or entity who acts in good faith reliance on a governmental request pursuant to Section 2703(f) also has a complete defense to civil and criminal liability.

Finally, the bill authorizes construction and operation of a National Cyber Crime Technical Support Center and 10 regional computer forensic labs that will provide education, training, and forensic examination capabilities for State and local law enforcement officials charged with investigating computer crimes. The section authorizes a total of $100 million for FY 2001, of which $20 million shall be available solely for the 10 regional labs and would complement the state computer crime grant bill, S. 1314, with which this bill is offered.

I am pleased to see the ''Protecting Seniors from Fraud Act'' pass as an amendment to this legislation. I was an original cosponsor of this bill, S. 3164, which Senator BAYH introduced on October 5, 2000, with Senators GRAMS and CLELAND. I have been concerned for some time that even as the general crime rate has been declining steadily over the past eight years, the rate of crime against the elderly has remained unchanged. That is why I introduced the Seniors Safety Act, S. 751, with Senators DASCHLE, KENNEDY, and TORRICELLI over a year ago.

The Protecting Seniors from Fraud Act includes one of the titles from the Seniors Safety Act. This title does two things. First, it instructs the Attorney General to conduct a study relating to crimes against seniors, so that we can develop a coherent strategy to prevent and properly punish such crimes. Second, it mandates the inclusion of seniors in the National Crime Victimization Study. Both of these are important steps, and they should be made law.

The Protecting Seniors from Fraud Act also includes important proposals for addressing the problem of crimes against the elderly, especially fraud crimes. In addition to the provisions described above, this bill authorizes the Secretary of Health and Human Services to make grants to establish local programs to prevent fraud against seniors and educate them about the risk of fraud, as well as to provide information about telemarketing and sweepstakes fraud to seniors, both directly and through State Attorneys General. These are two common-sense provisions that will help seniors protect themselves against crime.

I hope that we can also take the time to consider the rest of the Seniors Safety Act, and enact even more comprehensive protections for our seniors. The Seniors Safety Act offers a comprehensive approach that would increase law enforcement's ability to battle telemarketing, pension, and health care fraud, as well as to police nursing homes with a record of mistreating their residents. The Justice Department has said that the Seniors Safety Act would ''be of assistance in a number of ways.'' I have urged the Chairman of the Senate Judiciary Committee to hold hearings on the Seniors Safety Act as long ago as October 1999, and again this past February, but my requests have not been granted. Now, as the session is coming to a close, we are out of time for hearings on this important and comprehensive proposal and significant parts of the Seniors Safety Act remain pending in the Senate Judiciary Committee as part of the unfinished business of this Congress.

Let me briefly summarize the parts of the Seniors Safety Act that the majority in the Congress declined to consider. First, the Seniors Safety Act provides additional protections to nursing home residents. Nursing homes provide an important service for our seniors—indeed, more than 40 percent of Americans turning 65 this year will need nursing home care at some point in their lives. Many nursing homes do a wonderful job with a very difficult task—this legislation simply looks to protect seniors and their families by isolating the bad providers in operation. It does this by giving federal law enforcement the authority to investigate and prosecute operators of those nursing homes that engage in a pattern of health and safety violations. This authority is all the more important given the study prepared by the Department of Health and Human Services and reported this summer in the New York Times showing that 54 percent of American nursing homes fail to meet the Department's ''proposed minimum standard'' for patient care. The study also showed that 92 percent of nursing homes have less staff than necessary to provide optimal care.

Second, the Seniors Safety Act helps protect seniors from telemarketing fraud, which costs billions of dollars every year. This legislation would give the Attorney General the authority to block or terminate telephone service where that service is being used to defraud seniors. If someone takes your money at gunpoint, the law says we can take away their gun. If someone uses their phone to take away your money, the law should allow us to protect other victims by taking their phone away. In addition, this proposal would establish a Better Business Bureau-style clearinghouse that would keep track of complaints made about telemarketing companies. With a simple phone call, seniors could find out whether the company trying to sell to them over the phone or over the Internet has been the subject of complaints or been convicted of fraud. Senator BAYH has recently introduced another bill, S. 3025, the Combating Fraud Against Seniors Act, which includes the part of the Seniors Safety Act that establishes the clearinghouse for telemarketing fraud information.

Third, the Seniors Safety Act punishes pension fraud. Seniors who have worked hard for years should not have to worry that their hard-earned retirement savings will not be there when they need them. The bill would create new criminal and civil penalties for those who defraud pension plans, and increase the penalties for bribery and graft in connection with employee benefit plans.

Finally, the Seniors Safety Act strengthens law enforcement's ability to fight health care fraud. A recent study by the National Institute for Justice reports that many health care fraud schemes ''deliberately target vulnerable populations, such as the elderly or Alzheimer's patients, who are less willing or able to complain or alert law enforcement.'' This legislation gives law enforcement the additional investigatory tools it needs to uncover, investigate, and prosecute health care offenses in both criminal and civil proceedings. It also protects whistle-blowers who alert law enforcement officers to examples of health care fraud.

I commend Senators BAYH, GRAMS and CLELAND for working to take steps to improve the safety and security of America's seniors. We are doing the right thing today in passing this bipartisan legislation and beginning the fight to lower the crime rate against seniors. I also urge my colleagues to consider and pass the Seniors Safety Act. Taken together, these two bills would provide a comprehensive approach toward giving law enforcement and older Americans the tools they need to prevent crime.

On March 27, 2000, the Senate passed H.R. 1658, the Civil Asset Forfeiture Reform Act of 2000. This was an important step forward and I want to thank Mr. HYDE, Mr. CONYERS and Senators SESSIONS, BIDEN, SCHUMER and all others who worked with us in good faith to enact these long overdue reforms. At the same time, there was some unfinished business in connection with this legislation that a Hatch-Leahy amendment to H.R. 46 completes.

The bill that the Senate passed by unanimous consent on March 27th was supposed to be a substitute amendment to H.R. 1658. I had been led to believe that the substitute was word-for-word that which I had painstakingly worked out over the preceding weeks for approval by the Senate Committee on the Judiciary the previous Thursday, March 23, 2000. Imagine my surprise to see reprinted in the RECORD the next day a substitute amendment at variance with the version to which I had agreed to and at variance with the language that had been circulated to and approved by the Committee.

Specifically, the agreed upon version of the bill would amend section 983(a)(2)(C) of title 18, United States Code, to describe what a claimant in a civil asset forfeiture case must state to assert a claim. The amendment to which I agreed and which the Judiciary Committee ''ordered reported'' requires that a ''claim shall—(i) identify the specific property being claimed; (ii) state the claimant's interest in such property; and (iii) be made under oath, subject to penalty of perjury.''

By contrast, the version of the amendment submitted to the Senate for passage contained the following additional clause in subparagraph (ii): ''state the claimant's interest in such property (and provide customary documentary evidence of such interest if available) and state that the claim is not frivolous''. I did not approve the language inserted in the version considered by the Senate and this language was not approved by the Judiciary Committee.

This inserted language is superfluous, at best, since the claim must already be made under oath and penalty of perjury. At worst, this inserted language is an invitation for mischief in an area where the record has already amply demonstrated overreaching by law enforcement agencies. For example, if a claimant provides only partial paperwork supporting a claim to property seized by the government, would the claim be subject to dismissal for failure to state a claim? If a claimant certifies that the claim is not frivolous, as required by the inserted language, and a court ultimately determines otherwise, would the claimant be put at risk of a perjury prosecution? Even the threat of such risks puts additional burdens on claimants and may dissuade claimants from filing claims.

For these reasons, I had objected to insertion of this language and approved a substitute amendment that did not contain this problematic insert. Moreover, the version of that substitute amendment ''ordered reported'' by the Judiciary Committee and in the Committee's official files simply does not contain that problematic insert.

We rely every day on each other and on the professionalism of our staffs. Having raised my concern about the change as soon as it was discovered, I am pleased that Chairman HATCH has worked with me to pass a correction to the law that strikes the language that was added without agreement.

HERITAGE HARBOR MUSEUM NATIVE AMERICAN HISTORY

Mr. L. CHAFEE. Mr. President, today I rise to thank the chairman of the Senate Appropriations Subcommittee on Treasury and General Government, Senator CAMPBELL, for including funds for the National Historical Publications and Records Commission to provide a grant to the Heritage Harbor Museum in Providence for the development of the museum's Native American Story exhibit.