S. CON. RES. 162

Resolved by the Senate (the House of Representatives concurring), That the Clerk of the House of Representatives, in the enrollment of the bill (H.R. 4577), making appropriations for the Departments of Labor, Health and Human Services, and Education, and related agencies for the fiscal year ending September 2001, and for other purposes, shall make the following correction:

In section 1(a)(4), before the period at the end, insert the following: '', except that the text of H.R. 5666, as so enacted, shall not include section 123 (relating to the enactment of H.R. 4904)''.

Mr. STEVENS. Mr. President, I regret deeply that last concurrent resolution, and at some time in the future I will explain it.

I am awaiting some other papers. For the time being, let me say this. I have stood on the Senate floor several times talking about the Steller sea lion problem. I personally thank Mr. John Podesta, the President's assistant, for talking to me for so long and working with our staff and myself for so long, into the early hours this morning and through the day, to bring about a resolution of the problem I have been discussing.

I cannot say we won this argument, but I can say we have reached a conclusion that will allow a substantial portion, approximately 90 percent, of the fishermen affected by this issue to return to fishing next January. These are people who live along a stretch of coastline and on islands, as I said, that are the same distance as from this city to the end of the Florida chain. They are people who live in very harsh circumstances and have one basic source of income, and that is fishing.

We have been able now to agree on a process by which the fishing season will commence on January 20. Incidentally, it has nothing to do with the Inauguration; it just happens to be the first day of fishing season. We are delighted we have found a way to resolve the conflict. It still means there is a long hard task ahead of not only this Secretary of Commerce and his personnel but the next Secretary of Commerce and personnel to carry out the agreement we have crafted and to see that it works.

I am pleased to say we have had a great many people who have assisted us. As I said earlier, the distinguished majority leader and minority leader were personally involved, as were their staffs, along with the staff of the Assistant to the President, and the Office of Management and Budget. I cannot leave out, and would not leave out, the distinguished chairman of the House Appropriations Committee, the Honorable BILL YOUNG, a Representative from Florida, who waited for this resolution.

I know it was a harsh task he had, and there are many Members in both the House and Senate who were inconvenienced by this delay. I can only thank them for their cooperation. As I have said before, not one Member of Congress argued with me about the delay. They all understood that we had a substantial problem.

It is not easy to represent a State and people who live closer to Tokyo than Washington, DC. These people really have but three spokesmen in Washington compared to the many that other States have. They rely on us to convey their wishes and to convey their dilemmas over potential Federal actions and to seek solutions.

I am delighted we have received the cooperation that led to a consensus today that I believe will assist them and will start the resolution of this problem and bring it to a conclusion where we can abide by the Magnuson-Stevens Act that governs the fisheries off our shores and, at the same time, respect the findings that are made under the Endangered Species Act.

I thank Sylvia Matthews, Office of Management and Budget; Michael Deitch, Office of Management and Budget; Penny Dalton of NOAA; Mark Childress of Senator DASCHLE's office; Dave Hoppe of Senator LOTT's office; and Lisa Sutherland and David Russell of my office for their hard work on the issue pertaining to Steller sea lions.

PUBLIC SAFETY OFFICER MEDAL OF VALOR ACT OF 2000

Mr. STEVENS. Mr. President, I ask unanimous consent that the Judiciary Committee be discharged from further consideration of H.R. 46 and the Senate proceed to its immediate consideration.

The PRESIDING OFFICER. Without objection, it is so ordered. The clerk will report the bill by title.

The assistant legislative clerk read as follows:

A bill (H.R. 46) to provide a national medal for public safety officers who act with extraordinary valor above and beyond the call of duty.

There being no objection, the Senate proceeded to consider the bill.

Mr. LEAHY. Mr. President, today we consider three bipartisan measures 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; and a Hatch-Leahy-Schumer ''Internet Security 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 Act. I cosponsored the Stevens bill, S. 39, to establish a Public Safety Medal of Valor. 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.

On May 18, 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 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 most of 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, and sending it back to the House.

I have worked with Senator HATCH, Senator STEVENS and others to perfect the final version of this bill. We have crafted bipartisan improvements to ensure that the Medal of Valor Board will worked effectively and efficiently with the National Medal of Valor Office within the Department of Justice. Our legislation establishes both of these entities and it is essential that they work well together to design the Medal of Valor and to create the criteria and procedures for recommendations of nominees for the award. The men and women who will be honored by the Medal of Valor for their brave deeds deserve nothing less.

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 originally 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 though 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, section 303(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. Current law does not contain a definition of ''loss,'' which is being added by this amendment.

To take account of both the new definition of ''loss'' and the incorporation of the requisite jurisdictional thresholds into the description of the offense (rather than the current definition of ''damage''), the amendment to subsection (g) makes several changes. First, 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.

Second, the amendment clarifies that civil actions under section 1030, and not just 1030(a)(5), are limited to conduct that involves one of the factors enumerated in new subsection (a)(5)(B), namely, 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. This clarification is consistent with judicial constructions of the statute, requiring proof of the $5,000 loss threshold as a prerequisite for civil suit, for example, under subsection 1030(a)(2)(C). See, e.g., *America Online, Inc.* v. *LCGM, Inc.*, 46 F.Supp. 2d 444, 450 (E.D. Va. 1998) (court granted summary judgment on claim under 1030(a)(2)(C), stating, ''[p]laintiff asserts that as a result of defendants' actions, it suffered damages exceeding $5,000, the statutory threshold requirement'').

While proof of ''loss'' is required, this amendment preserves current law that civil enforcement of certain violations of section 1030 is available without requiring proof of ''damage,'' which is defined in the amendment to mean ''any impairment to the integrity or availability of data, a program, a system, or information.'' In fact, only subsection 1030(a)(5) requires proof of ''damage''; civil enforcement of other subsections of this law may proceed without such proof. Thus, only the factors enumerated in new subsection (a)(5)(B), and not its introductory language referring to conduct described in subsection (a)(5)(A), constitute threshold requirements for civil suits for violations of section 1030 other than subsection 1030(a)(5).

Finally, the amendment adds a new sentence to subsection 1030(g) clarifying that civil actions may not be brought ''for the negligent design or manufacture of computer hardware, computer software, or firmware.''

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. 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 to subsection 1030(g) is intended to ensure that the civil remedy is a robust option for private enforcement actions, while limiting its applicability to negligence cases that are more appropriately governed by contractual warranties, state tort law and consumer protection laws.

Fifth, sections 304 and 309 of the Hatch-Leahy-Schumer Internet Security Act amendment to H.R. 46 authorize criminal 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 309 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 criminal forfeiture provision in section 304 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 304 and 309 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 304 and 309. 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 304 and 309 make it more difficult for the government to prove that the property should be forfeited.

Sixth, 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, 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.

Eighth, section 310 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 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.

Ninth, 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).

Under current law, 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).

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 relating to its jurisdiction under 18 U.S.C. § 3056 and subject to agreement between the Secretary of the Treasury and the Attorney General. This provision also makes clear that the FBI retains primary authority to investigate offenses under subsection 1030(a)(1).

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. This arrangement is consistent with other jurisdictional grants of authority to the Secret Service. See, e.g., 18 U.S.C. §§ 1029(d), 3056(b)(3).

Tenth, section 307 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 307 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.

AMENDMENT NO. 4366

(Purpose: To enhance computer crime enforcement and Internet security, and for other purposes)

Mr. STEVENS. Mr. President, Senator HATCH has an amendment which is at the desk.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS], for Mr. HATCH, proposes an amendment numbered 4366.

(The text of the amendment is printed in today's RECORD under ''Amendments Submitted.'')

Mr. STEVENS. Mr. President, I ask unanimous consent that the amendment be agreed to.

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

The amendment (No. 4366) was agreed to.

Mr. STEVENS. Mr. President, I ask unanimous consent that the bill, as amended, be read the third time and passed, the motion to reconsider be laid upon the table, the amendment to the title be agreed to, and any statements relating to the bill be printed in the RECORD.

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

The bill (H.R. 46), as amended, was read the third time and passed.

The title was amended so as to read:

To provide a national medal for public safety officers who act with extraordinary valor above and beyond the call of duty, to enhance computer crime enforcement and Internet security, and for other purposes.

MAKING TECHNICAL CORRECTIONS

Mr. STEVENS. Mr. President, I ask unanimous consent that the Judiciary