her sole discretion, extend such effective date up to an additional six months. Notwithstanding any other provision of law, the decision of the Attorney General on such an application shall not be subject to judicial review.

SEC. 402. MAIL ORDER RESTRICTIONS.

Section 310(b) of the Controlled Substances Act (21 U.S.C. 830(b)) is amended by adding at the end the following:

''(3) MAIL ORDER REPORTING.—(A) Each regulated person who engages in a transaction with a nonregulated person which—

''(i) involves ephedrine, pseudoephedrine, or phenylpropanolamine (including drug products containing these chemicals); and

''(ii) uses or attempts to use the Postal Service or any private or commercial carrier;

shall, on a monthly basis, submit a report of each such transaction conducted during the previous month to the Attorney General in such form, containing such data, and at such times as the Attorney General shall establish by regulation.

''(B) The data required for such reports shall include—

''(i) the name of the purchaser;

''(ii) the quantity and form of the ephedrine, pseudoephedrine, or phenylpropanolamine purchased; and

''(iii) the address to which such ephedrine, pseudoephedrine, or phenylpropanolamine was sent.''.

TITLE V—EDUCATION AND RESEARCH

SEC. 501. INTERAGENCY METHAMPHETAMINE TASK FORCE.

(a) ESTABLISHMENT.—There is established a ''Methamphetamine Interagency Task Force'' (referred to as the ''interagency task force'') which shall consist of the following members:

(1) The Attorney General, or a designee, who shall serve as chair.

(2) 2 representatives selected by the Attorney General.

(3) The Secretary of Education or a designee.

(4) The Secretary of Health and Human Services or a designee.

(5) 2 representatives of State and local law enforcement and regulatory agencies, to be selected by the Attorney General.

(6) 2 representatives selected by the Secretary of Health and Human Services.

(7) 5 nongovernmental experts in drug abuse prevention and treatment to be selected by the Attorney General.

(b) RESPONSIBILITIES.—The interagency task force shall be responsible for designing, implementing, and evaluating the education and prevention and treatment practices and strategies of the Federal Government with respect to methamphetamine and other synthetic stimulants.

(c) MEETINGS.—The interagency task force shall meet at least once every 6 months.

(d) FUNDING.—The administrative expenses of the interagency task force shall be paid out of existing Department of Justice appropriations.

(e) FACA.—The Federal Advisory Committee Act (5 U.S.C. App. 2) shall apply to the interagency task force.

(f) TERMINATION.—The interagency task force shall terminate 4 years after the date of enactment of this Act.

SEC. 502. PUBLIC HEALTH MONITORING.

The Secretary of Health and Human Services shall develop a public health monitoring program to monitor methamphetamine abuse in the United States. The program shall include the collection and dissemination of data related to methamphetamine abuse which can be used by public health officials in policy development.

SEC. 503. PUBLIC-PRIVATE EDUCATION PROGRAM.

(a) ADVISORY PANEL.—The Attorney General shall establish an advisory panel consisting of an appropriate number of representatives from Federal, State, and local law enforcement and regulatory agencies with experience in investigating and prosecuting illegal transactions of precursor chemicals. The Attorney General shall convene the panel as often as necessary to develop and coordinate educational programs for wholesale and retail distributors of precursor chemicals and supplies.

(b) CONTINUATION OF CURRENT EFFORTS.—The Attorney General shall continue to—

(1) maintain an active program of seminars and training to educate wholesale and retail distributors of precursor chemicals and supplies regarding the identification of suspicious transactions and their responsibility to report such transactions; and

(2) provide assistance to State and local law enforcement and regulatory agencies to facilitate the establishment and maintenance of educational programs for distributors of precursor chemicals and supplies.

SEC. 504. SUSPICIOUS ORDERS TASK FORCE.

(a) IN GENERAL.—The Attorney General shall establish a ''Suspicious Orders Task Force'' (the ''Task Force'') which shall consist of—

(1) appropriate personnel from the Drug Enforcement Administration (the ''DEA'') and other Federal, State, and local law enforcement and regulatory agencies with the experience in investigating and prosecuting illegal transactions of listed chemicals and supplies; and

(2) representatives from the chemical and pharmaceutical industry.

(b) RESPONSIBILITIES.—The Task Force shall be responsible for developing proposals to define suspicious orders of listed chemicals, and particularly to develop quantifiable parameters which can be used by registrants in determining if an order is a suspicious order which must be reported to DEA. The quantifiable parameters to be addressed will include frequency of orders, deviations from prior orders, and size of orders. The Task Force shall also recommend provisions as to what types of payment practices or unusual business practices shall constitute prima facie suspicious orders. In evaluating the proposals, the Task Force shall consider effectiveness, cost and feasibility for industry and government, an other relevant factors.

(c) MEETINGS.—The Task Force shall meet at least two times per year and at such other times as may be determined necessary by the Task Force.

(d) REPORT.—The Task Force shall present a report to the Attorney General on its proposals with regard to suspicious orders and the electronic reporting of suspicious orders within one year of the date of enactment of this Act. Copies of the report shall be forwarded to the Committees of the Senate and House of Representatives having jurisdiction over the regulation of listed chemical and controlled substances.

(e) FUNDING.—The administrative expenses of the Task Force shall be paid out of existing Department of Justice funds or appropriations.

(f) FACA.—The Federal Advisory Committee Act (5 U.S.C. App. 2) shall apply to the Task Force.

(g) TERMINATION.—The Task Force shall terminate upon presentation of its report to the Attorney General, or two years after the date of enactment of this Act, whichever is sooner.

MEASURE READ THE FIRST TIME—SENATE JOINT RESOLUTION 61

Mr. STEVENS. Mr. President, I send to the desk a joint resolution on behalf of Senators THURMOND and HEFLIN and ask for its first reading.

The PRESIDING OFFICER. The clerk will read the joint resolution for the first time.

A joint resolution (S.J. Res. 61) regarding the Emergency Management Assistant Compact.

Mr. STEVENS. Mr. President, I now ask for second reading, and I object to my own request on behalf of the other side of the aisle.

The PRESIDING OFFICER. The bill will be read on the next legislative day.

ECONOMIC ESPIONAGE ACT

Mr. STEVENS. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of H.R. 3723, which is now at the desk.

The PRESIDING OFFICER. The clerk will report the bill.

The assistant legislative clerk read as follows:

A bill (H.R. 3723) to amend Title 18 U.S. Code to protect proprietary economic information, and for other purposes.

The PRESIDING OFFICER. Is there objection to the immediate consideration of the bill?

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

AMENDMENT NO. 5384

(Purpose: To propose a substitute)

Mr. STEVENS. Mr. President, I send a substitute amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS] for Mr. SPECTER, for himself and Mr. KOHL, proposes an amendment numbered 5384.

Mr. STEVENS. Mr. President, I ask unanimous consent that reading of the amendment be dispensed with.

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

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

AMENDMENT NO. 5385 TO AMENDMENT NO. 5384

(Purpose: To amend title 18, United States Code, to prohibit certain activities relating to the use of computers, and for other purposes)

Mr. STEVENS. Mr. President, I send an amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS], for Mr. GRASSLEY, for himself and Mr. KYL, proposes an amendment numbered 5385 to Amendment No. 5384.

Mr. STEVENS. Mr. President, I ask unanimous consent that reading of the amendment be dispensed with.

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

The amendment is as follows:

At the appropriate place, add the following new section: Sec. 6.

(a) WIRE AND COMPUTER FRAUD.—Section 1343 of title 18, United States Code, is amended——

(1) by adding at the end the following new subsection:

''(b) SECRET SERVICE JURISDICTION.—''The Secretary of the Treasury and the Attorney General are authorized to enter into an agreement under which the United States Secret Service may investigate certain offenses under this section.''

(a) USE OF CERTAIN TECHNOLOGY TO FACILITATE CRIMINAL CONDUCT.——

(1) INFORMATION.—The Administrative Office of the United States Courts shall establish policies and procedures for the inclusion in all Presentence Reports of information that specifically identifies and describes any use of encryption or scrambling technology that would be relevant to an enhancement under Section 3C1.1 (dealing with Obstructing or Impeding the Administration of Justice) of the Sentencing Guidelines or to offense conduct under the Sentencing Guidelines.

(2) COMPILING AND REPORT.—The United States Sentencing Commission shall——

(A) compile and analyze any information contained in documentation described in paragraph (1) relating to the use of encryption or scrambling technology to facilitate or conceal criminal conduct; and

(B) based on the information compiled and analyzed under subparagraph (A), annually report to the Congress on the nature and extent of the use of encryption or scrambling technology to facilitate or conceal criminal conduct.''

(c) Section 1029 of Title 18, United States Code is amended by—''Striking the (a)(5) in the second place it appears and replacing it with (a)(8); by striking the (a)(6) the second place it appears and replacing it with (a)(9); and by adding the following new section:

''(a)(10) knowingly and with intent to defraud uses, produces, traffics in, or possesses any device containing electronically stored monetary value.''

Mr. GRASSLEY. Mr. President, I'm pleased that the Senate has passed the eonomic espionage bill. This is an important measure that I believe will save American business significant amounts of money. The theft of confidential information from American businesses is a serious problem, and this bill takes important steps in the right direction.

I am particularly pleased that the Senate has accepted the amendment I offered with Senator KYL. This amendment commissions the first-ever study on the criminal misuse of encryption technologies. Under the Grassley-Kyl amendment, court officers who prepare pre-sentencing reports will include information on the use of encryption to conceal criminal conduct, obstruct investigations, and commit crimes. The sentencing commission will then collect and collate this information and include it in its annual report to congress.

In this way, I am hopeful that Congress and executive branch will have reliable data on whether the criminal misuse of encryption is actually a problem and, if so, what response to this problem would be appropriate.

As chairman of the Oversight Subcommittee on the Judiciary Committee, I did an informal survey of state-level law enforcement concerning the criminal misuse of encryption. This informal survey, while not scientific, provides valuable insights into the actions of the criminal element in our society.

Here are just some of the responses my subcommittee received.

In one case involving John Lucich of the New Jersey attorney general's office was involved, a computer was seized pursuant to a warrant in a serious assault case. Examination revealed that approximately 20 percent of the hard drive files were encrypted. Investigators sought the assistance of two different Federal agencies. Both of these agencies were unsuccessful in decrypting the files. Finally, a third Federal agency was successful in decrypting the files after expending considerable resources. The Decrypted files did not contain evidence of the assault but rather contained evidence of child pornography. The encryption type likely used was ''DES.''

And Officer Tim O'Neill of the Roseville, California Police Department reported to the subcommittee that he participated in a search involving a complaint against a subject who was on probation for solicitation/annoyance of minors. The subject had a hidden encrypted file on his personal computer. In the ''slack'' area at the end of the file the officer found names, addresses, school, grade, and phone numbers of 4–5 young teen girls. The encryption type used was known as ''pincrypt.''

Officer Mike Menz of the same department advised the subcommittee that he was working on a joint State/Federal major check fraud case where part of the potential evidence was encrypted.

Ivan Ortman, a senior prosecutor in Seattle, Washington, encountered some encrypted files and password protection in a cellular phone fraud investigation. For a number of files the popular and inexpensive ''PGP'' type of encryption was used. Orton indicated that no effort was even made to examine the files as the police could not locate any method for ''cracking that encryption.''

In other words, why try since such an effort is certain to be futile. Surely a rational society should look long and hard at this situation.

Agent Chuck Davis of the Colorado Bureau of Investigation reported to the subcommittee that he has encountered encryption as well as password protection problems. In one embezzlement case, a computer system has seized. Examination revealed that files on the hard disk were encrypted. The software manufacturers were contacted and the technical personnel who wrote the program advised that, ''they had left no 'back door' access to the product as this would adversely impact sales. The hallmark of the program's appeal is that it cannot be broken, even by those who created it.'' Agent Davis advised that his investigation was ''halted'' due to the time and expense of a ''brute force attack''. The encryption program used was entitled ''watchdog.''

Agent Davis also advised the subcommittee that password protection also presents problems for other types of investigators. In cases involving theft of drugs from an emergency room by a doctor, bribery/extortion by a police officer, and the suicide by an 11 year-old boy after telling friends that he had been molested by a family friend, investigators encountered password protection. The first two cases were successfully resolved through assistance from the manufacturer of the software.

The third case, however, especially illustrates the seriousness of decryption problems—determining the unique key or in this case, password from a large number of possibilities. According to Agent Davis, a mere 4 character password has 1.9 million possibilities due to the number of keyboard characters. Can you imagine how difficult it must be to figure a short, 4 character password. What if the password were 10 characters or 20 or more? It's easy to see why criminals are moving toward password protection for their records.

Mr. President, I don't know what the Grassley-Kyl amendment's study will show. But at least anecdotally, there seems to be a serious and growing problem with criminals using encryption to commit crimes or conceal criminal conduct. I hope we can figure out what to do about the problem in a fair and balanced way. I yield the floor.

Mr. KYL. Mr. President, I rise to comment on the economic espionage bill introduced by Senators SPECTER and KOHL. I was pleased that the Senate Judiciary Committee passed this bill, which will strengthen current public law on crimes against our industries. It will protect our businesses by punishing those who steal vital proprietary information for the benefit of a foreign government or a corporation.

Economic espionage is not a new crime. The success of many U.S. firms has made them a large target for the theft of trade secrets. It is much easier for a foreign firm to steal American trade secrets, with little or no penalty, than it is for a firm to spend a large amount of capital on research and development. Economic espionage may be the future of intelligence.

Only recently have American firms begun to recognize the economic impact espionage has on U.S. firms. In 1992, a survey by the American society for Industrial Security discovered that American firms lost roughly $597 million in product development and specification data and $110 million in manufacturing process information, due to espionage. These losses are likely to continue. I am pleased that the Chairman and ranking member have produced a bill that will for the first time

penalize those who try to steal ideas that Americans have worked hard to develop.

One problem not yet adequately addressed is how to collect necessary intelligence in an age when encryption protects computer communication. In order to maintain our national security interests, I support some measure of constitutional authority to collect intelligence even in situations where communications have been encrypted. To that end, Mr. President, I am hopeful that my colleagues will adopt an amendment to this bill that Senator GRASSLEY and I have sponsored. It will amend the federal sentencing guidelines to require that the Federal Sentencing Commission collect, compile, and report annually on information collected from pretrial sentence reports and other relevant documents indicating the use of encryption to further or conceal criminal conduct.

Whatever one's view of export policy, it is clear that law enforcement must have better records of criminals who use encryption technology. This amendment will accomplish that.

Mr. President, passing an economic espionage law will deter criminals from stealing trade secrets from American businesses. I urge my colleagues to adopt our amendment and pass the bill.

The PRESIDING OFFICER. The question is on agreeing to the amendment.

The amendment (No. 5385) was agreed to.

Mr. GRASSLEY. I am pleased that the amendment I offered with my good friend Senator KYL has been accepted. This amendment requires the Sentencing Commission to report to Congress every year on the criminal misuse of encryption technologies, including to obstruct or impede the administration of justice. I think that this will help Congress obtain reliable data on the question of whether encryption is actually being used by criminals to commit crimes.

The Grassley-Kyl amendment also provides the Attorney General and Secretary of the Treasury with the authority to enter into an agreement providing the United States Secret Service with concurrent jurisdiction to investigate certain types of wire fraud offenses. I considered amending 18 U.S.C. 1343 to specifically encompass computer frauds, but after reviewing the case law (see, *E.G., U.S.* v. *Riggs*, 967 F.2d 561 (11th Cir. 1992)) and consulting with the Justice Department, I have decided that this is not necessary. My hope is that Federal law enforcement and the Justice Department will make more use of section 1343 to prosecute computer crimes. Specifically, I would like this interpretation to be committed to writing and distributed to Federal prosecutors in the field.

Mr. LEAHY. I concur in the view of the Senator from Iowa that amending section 1343 as he originally considered is not necessary. Section 1343 already encompasses frauds effected by the interstate or foreign transmission of wire communications involving, among other things, writings, signs, or signals and, consequently, would encompass frauds effected by means of computers in interstate or foreign commerce. I know the Justice Department already interprets 1343 in this way. I too would urge the Justice Department to ensure that Federal prosecutors in the field are familiar with the scope of criminal conduct, including fraud effected by means of computers, encompassed by the wire fraud statute.

Regarding the new requirement that the Sentencing Commission report on the criminal misuse of encryption technologies. I caution that the results of this report—whatever they may be—will be necessarily incomplete and should not be viewed out of context. Instances in which encryption technologies have been used to thwart the theft of valuable computerized data, which has been encrypted, and to prevent crimes, such as economic espionage, do not usually draw the attention of law enforcement and therefore will not be included in the report.

Mr. GRASSLEY. I wonder whether the chairman and ranking member of the Technology Subcommittee agree with this analysis of section 1343.

Mr. SPECTER. I have listened to your exchange with Senator LEAHY and I fully agree that section 1343 already encompasses computer fraud and that amending it is not necessary.

Mr. KOHL. I too listened to your exchange with Senator LEAHY, and I am also of the view that section 1343 covers some computer crimes and that no amendment was necessary.

AMENDMENT NO. 5386

(Purpose: To improve the treatment and security of certain persons found not guilty by reason of insanity in the District of Columbia, and for other purposes)

Mr. STEVENS. Mr. President, I send an amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS], for Mr. HATCH, proposes an amendment numbered 5386.

Mr. STEVENS. Mr. President, I ask unanimous consent that reading of the amendment be dispensed with.

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

The amendment is as follows:

At the appropriate place in the bill, add the following:

SEC. . TRANSFER OF PERSONS FOUND NOT GUILTY BY REASON OF INSANITY.

(a) AMENDMENT OF SECTION 4243 OF TITLE 18.—Section 4243 of title 18, United States Code, is amended by adding at the end the following new subsection:

''(i) CERTAIN PERSONS FOUND NOT GUILTY BY REASON OF INSANITY IN THE DISTRICT OF COLUMBIA.—

''(1) TRANSFER TO CUSTODY OF THE ATTORNEY GENERAL.—Notwithstanding section 301(h) of title 24 of the District of Columbia Code, and notwithstanding subsection 4247(j) of this title, all persons who have been committed to a hospital for the mentally ill pursuant to section 301(d)(1) of title 24 of the District of Columbia Code, and for whom the United States has continuing financial responsibility, may be transferred to the custody of the Attorney General, who shall hospitalize the person for treatment in a suitable facility.

''(2) APPLICATION.—

''(A) IN GENERAL.—The Attorney General may establish custody over such persons by filing an application in the United States District Court for the District of Columbia, demonstrating that the person to be transferred is a person described in this subsection.

''(B) NOTICE.—The Attorney General shall, by any means reasonably designed to do so, provide written notice of the proposed transfer of custody to such person or such person's guardian, legal representative, or other lawful agent. The person to be transferred shall be afforded an opportunity, not to exceed 15 days, to respond to the proposed transfer of custody, and may, at the court's discretion, be afforded a hearing on the proposed transfer of custody. Such hearing, if granted, shall be limited to a determination of whether the constitutional rights of such person would be violated by the proposed transfer of custody.

''(C) ORDER.—Upon application of the Attorney General, the court shall order the person transferred to the custody of the Attorney General, unless, pursuant to a hearing under this paragraph, the court finds that the proposed transfer would violate a right of such person under the United States Constitution.

''(D) EFFECT.—Nothing in this paragraph shall be construed to—

''(i) create in any person a liberty interest in being granted a hearing or notice on any matter;

''(ii) create in favor of any person a cause of action against the United States or any officer or employee of the United States; or

''(iii) limit in any manner or degree the ability of the Attorney General to move, transfer, or otherwise manage any person committed to the custody of the Attorney General.

''(3) CONSTRUCTION WITH OTHER SECTIONS.—Subsections (f) and (g) and section 4247 shall apply to any person transferred to the custody of the Attorney General pursuant to this subsection.''.

(b) TRANSFER OF RECORDS.—Notwithstanding any provision of the District of Columbia Code or any other provision of law, the District of Columbia and St. Elizabeth's Hospital—

(1) not later than 30 days after the date of enactment of this Act, shall provide to the Attorney General copies of all records in the custody or control of the District or the Hospital on such date of enactment pertaining to persons described in section 4243(i) of title 18, United States Code (as added by subsection (a));

(2) not later than 30 days after the creation of any records by employees, agents, or contractors of the District of Columbia or of St. Elizabeth's Hospital pertaining to persons described in section 4243(i) of title 18, United States Code, provide to the Attorney General copies of all such records created after the date of enactment of this Act;

(3) shall not prevent or impede any employee, agent, or contractor of the District of Columbia or of St. Elizabeth's Hospital who has obtained knowledge of the persons described in section 4243(i) of title 18, United States Code, in the employee's professional capacity from providing that knowledge to the Attorney General, nor shall civil or criminal liability attach to such employees, agents, or contractors who provide such knowledge; and

(4) shall not prevent or impede interviews of persons described in section 4243(i) of title 18, United States Code, by representatives of the Attorney General, if such persons voluntarily consent to such interviews.

(c) CLARIFICATION OF EFFECT ON CERTAIN TESTIMONIAL PRIVILEGES.—The amendments made by this section shall not be construed to affect in any manner any doctor-patient or psychotherapist-patient testimonial privilege that may be otherwise applicable to persons found not guilty by reason of insanity and affected by this section.

(d) SEVERABILITY.—If any provision of this section, an amendment made by this section, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this section and the amendments made by this section shall not be affected thereby.

The PRESIDING OFFICER. The question is on agreeing to the amendment.

The amendment (No. 5386) was agreed to.

AMENDMENT NO. 5387 TO AMENDMENT NO. 5384

(Purpose: To provide funding for the establishment of Boys and Girls Clubs in public housing projects and other distressed areas, and for other purposes)

Mr. STEVENS. Mr. President, I send an amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS], for Mr. HATCH, for himself, and Mr. KOHL, proposes an amendment numbered 5387 to amendment No. 5384.

Mr. STEVENS. Mr. President, I ask unanimous consent that reading of the amendment be dispensed with.

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

The amendment is as follows:

At the appropriate place in the bill, add the following:

SEC. . ESTABLISHING BOYS AND GIRLS CLUBS.

(a) FINDINGS AND PURPOSE.—

(1) FINDINGS.—The Congress finds that—

(A) the Boys and Girls Clubs of America, chartered by an Act of Congress on December 10, 1991, during its 90-year history as a national organization, has proven itself as a positive force in the communities it serves;

(B) there are 1,810 Boys and Girls Clubs facilities throughout the United States, Puerto Rico, and the United States Virgin Islands, serving 2,420,000 youths nationwide;

(C) 71 percent of the young people who benefit from Boys and Girls Clubs programs live in our inner cities and urban areas;

(D) Boys and Girls Clubs are locally run and have been exceptionally successful in balancing public funds with private sector donations and maximizing community involvement;

(E) Boys and Girls Clubs are located in 289 public housing sites across the Nation;

(F) public housing projects in which there is an active Boys and Girls Club have experienced a 25 percent reduction in the presence of crack cocaine, a 22 percent reduction in overall drug activity, and a 13 percent reduction in juvenile crime;

(G) these results have been achieved in the face of national trends in which overall drug use by youth has increased 105 percent since 1992 and 10.9 percent of the Nation's young people use drugs on a monthly basis; and

(H) many public housing projects and other distressed areas are still underserved by Boys and Girls Clubs.

(2) PURPOSE.—It is the purpose of this section to provide adequate resources in the form of seed money for the Boys and Girls Clubs of America to establish 1,000 additional local Boys and Girls Clubs in public housing projects and other distressed areas by 2001.

(b) DEFINITIONS.—For purposes of this section—

(1) the terms ''public housing'' and ''project'' have the same meanings as in section 3(b) of the United States Housing Act of 1937; and

(2) the term ''distressed area'' means an urban, suburban, or rural area with the high percentage of high risk youth as defined in section 509A of the Public Health Service Act (42 U.S.C. 290aa–8(f)).

(c) ESTABLISHMENT.—

(1) IN GENERAL.—For each of the fiscal years 1997, 1998, 1999, 2000, and 2001, the Director of the Bureau of Justice Assistance of the Department of Justice shall provide a grant to the Boys and Girls Clubs of America for the purpose of establishing Boys and Girls Clubs in public housing projects and other distressed areas.

(2) CONTRACTING AUTHORITY.—Where appropriate, the Secretary of Housing and Urban Development, in consultation with the Attorney General, shall enter into contracts with the Boys and Girls Clubs of America to establish clubs pursuant to the grants under paragraph (1).

(d) REPORT.—Not later than May 1 of each fiscal year for which amounts are made available to carry out this Act, the Attorney General shall submit to the Committees on the Judiciary of the Senate and the House of Representatives a report that details the progress made under this Act in establishing Boys and Girls Clubs in public housing projects and other distressed areas, and the effectiveness of the programs in reducing drug abuse and juvenile crime.

(e) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated to carry out this section—

(A) $20,000,000 for fiscal year 1997;

(B) $20,000,000 for fiscal year 1998;

(C) $20,000,000 for fiscal year 1999;

(D) $20,000,000 for fiscal year 2000; and

(E) $20,000,000 for fiscal year 2001;

(2) VIOLENT CRIME REDUCTION TRUST FUND.—The sums authorized to be appropriated by this subsection may be made from the Violent Crime Reduction Trust Fund.

The PRESIDING OFFICER. The question is on agreeing to the amendment.

The amendment (No. 5387) was agreed to.

Mr. STEVENS. Mr. President, I ask unanimous consent that the substitute, as amended, be agreed to, the bill be deemed read the third time, and passed, the motion to reconsider be laid upon the table, and that any statements relating to the bill appear at this point in the RECORD.

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

The committee substitute amendment was agreed to.

The bill (H.R. 3723), as amended, was passed.

Mr. KOHL. Mr. President, I am pleased that today the Senate has taken up and passed H.R. 3723. We are sending that bill back to the House with substitute. This language, which I drafted with Senator SPECTER, is based on our companion measures, S. 1556 (''The Economic Espionage Act'') and S.1557 (''The Economic Security Act'').

I would like to take this opportunity to point out several provisions of our legislation and explain their purpose and meaning.

This legislation includes a provision penalizing the theft of proprietary economic information and a second provision penalizing that theft when it is done on behalf of or to benefit a foreign government, instrumentality, or agent. The principle purpose of this second (foreign government) provision is not to punish conventional commercial theft and misappropriation of trade secrets (which is covered by the first provision). Thus, to make out an offense under this section, the prosecution must show in each instance that the perpetrator intended to, or had reason to believe that his or her actions would aid a foreign government, instrumentality, or agent. Enforcement agencies should administer this section with its principle purpose in mind and therefore should not apply section 572 to foreign corporations when there is no evidence of foreign government sponsored or coordinated intelligence activity. This particular concern is borne out in our understanding of the definition of ''foreign instrumentality,'' which indicates that a foreign organization must be ''substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government or subdivision thereof.'' We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

To make out a case under these two provisions (sections 1832 and 572), the prosecution would have to show that the accused knew or had reason to know that a trade secret had been stolen or appropriated without authorization. This threshold separates conduct that is criminal from that which is innocent. Thus, for example, these sections would not give rise to prosecution for legitimate economic collection or reporting by personnel of foreign governments or international financial institutions, such as the World Bank, because such legitimate collection or reporting would not include the collection or reporting of trade secrets that had been stolen, misappropriated or converted without authorization.

In the section dealing with foreign government sponsored espionage, and derived from S. 1557, the definition of proprietary economic information is different from the definition of proprietary economic information in section 2. In particular, the definition contained in section 1831(2) indicates that ''general knowledge'' is not included in the term, while the definition in section 571(4) does not. We do not intend

to imply by this difference that general knowledge can or should be the subject of a prosecution under section 572. Of course, someone can use their general experience and skills and work for a foreign government. They cannot, however, steal a piece of proprietary economic information for an owner and thereby violate section 572 of this provision. Our point is simply that when a person is working on behalf of a foreign government, instrumentality or agency, that person has to be particularly careful to ensure that the information being used is not proprietary economic information.

Some people have asked whether a piece of proprietary economic information has to be novel or inventive. Unlike patented material, something does not have to be novel, in the patent law sense, in order to be a piece of proprietary economic information. Of course, often it will be because an owner will have a patented invention that he or she has chosen to maintain the material as a piece of proprietary economic information rather than reveal it through the patent process. Even if the material is not novel in the patent law sense, some form of novelty is probably inevitable since ''that which does not possess novelty is usually known; secrecy, in the context of trade secrets implies at least minimal novelty.'' *Kewanee Oil Co.* v. *Bicron Corp.*, 416 U.S. 470, 476 (1974). While we do not strictly impose a novelty or inventiveness requirement in order for material to be considered proprietary economic information, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience.

Although we do not require novelty or inventiveness, the definition of proprietary economic information includes the provision that an owner have taken reasonable measures under the circumstances to keep the information confidential. We do not with this definition impose any requirements on companies or owners. Each owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be. We anticipate that what constitutes reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry. However, some common sense measures are likely to be common across the board. For example, it is only natural that an owner would restrict access to proprietary economic information to the people who actually need to use the information. It is only natural also that an owner clearly indicate in some form or another that the information is proprietary. However, owners need not take heroic or extreme protective measures in order for their efforts to be reasonable.

Some people have asked how this legislation might affect reverse engineering. Reverse engineering is a broad term that encompasses a variety of actions. The important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has ''reverse engineered.'' If someone has lawfully gained access to a trade secret or a piece or proprietary economic information, and can replicate it without violating copyright, patent or this law, then that form of ''reverse engineering'' should be fine. For example, if a person can drink Coca-Cola and, because he happens to have highly refined taste buds, can figure out what the formula is, then this legislation cannot be used against him. Likewise, if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product, then that person should be free from any threat of prosecution.

We have been deeply concerned about the efforts taken by courts to protect the confidentiality of proprietary economic information. It is important that in the early stages of a prosecution the issue whether material is proprietary economic information not be litigated. Rather, courts should, when entering these orders, always assume that the material at issue is in fact proprietary economic information.

We are also concerned that victims of economic espionage receive compensation for their losses. This legislation incorporates through reference existing law to provide procedures to be used in the detention, seizure, forfeiture, and ultimate disposition of property forfeited under the section. Under these procedures, the Attorney General is authorized to grant petitions for mitigation or remission of forfeiture and for the restoration of forfeited property to the victims of an offense. The Attorney General may also take any other necessary or proper action to protect the rights of innocent people in the interest of justice. In practice, under the forfeiture laws, victims are afforded priority in the disposition of forfeited property since it is the policy of the Department of Justice to provide restitution to the victims of criminal acts whenever permitted to do so by the law. Procedures for victims to obtain restitution may be found at Section 9 of Title 28, Code of Federal Regulations.

In addition to requesting redress from the Attorney General, any person—including a victim—asserting an interest in property ordered forfeited may petition for a judicial hearings to adjudicate the validity of the alleged interest and to revise the order of forfeiture. Additionally, forfeitures are subject to a requirement of proportionality under the Eight Amendment; that is, the value of the property forfeited must not be excessively disproportionate to the crimes in question.

Finally, we have required that the Attorney General report back to us on victim restitution two and four years after the enactment of this legislation. We have heard from some companies that they only rarely obtain restitution awards despite their eligibility. We wish to carefully monitor restitution to ensure that the current system is working well and make any changes that may be necessary.

Mr. President, we have worked closely in cooperation with the Administration in drafting this legislation. It is a bipartisan measure, broadly supported, and necessary for our country's future industrial vitality.

NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996

Mr. STEVENS. Mr. President, I ask unanimous consent the Senate now proceed to the consideration of Calendar No. 563, S. 982.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

A bill (S. 982) to protect the national information infrastructure, and for other purposes.

The PRESIDING OFFICER. Is there objection to the immediate consideration of the bill?

There being no objection, the Senate proceeded to consider the bill which had been reported from the Committee on the Judiciary, with an amendment to strike all after the enacting clause and inserting in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Information Infrastructure Protection Act of 1996''.

SEC. 2. COMPUTER CRIME.

Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''knowingly accesses'' and inserting ''having knowingly accessed'';

(ii) by striking ''exceeds'' and inserting ''exceeding'';

(iii) by striking ''obtains information'' and inserting ''having obtained information'';

(iv) by striking ''the intent or'';

(v) by striking ''is to be used'' and inserting ''could be used''; and

(vi) in inserting before the semicolon at the end the following: ''willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it'';

(B) in paragraph (2)—

(i) by striking ''obtains information'' and inserting ''obtains—

''(A) information''; and

(ii) by adding at the end the following new subparagraphs:

''(B) information from any department or agency of the United States; or

''(C) information from any protected computer if the conduct involved an interstate or foreign communication;'';

(C) in paragraph (3)—

(i) by inserting ''nonpublic'' before ''computer of a department or agency'';

(ii) by striking ''adversely''; and

(iii) by striking ''the use of the Government's operation of such computer'' and inserting