Friday, July 12, 2002 at 1:21 p.m., and said to contain a message from the President whereby he transmits the District of Columbia's Fiscal Year 2003 Budget Request Act.

Sincerely yours,

MARTHA C. MORRISON,
Deputy Clerk.

DISTRICT OF COLUMBIA FISCAL YEAR 2003 BUDGET REQUEST ACT—MESSAGE FROM THE PRESIDENT OF THE UNITED STATES (H. DOC. NO. 107–)

The SPEAKER pro tempore laid before the House the following message from the President of the United States; which was read and, together with the accompanying papers, without objection, referred to the Committee on Appropriations and ordered to be printed:

To the Congress of the United States:

Pursuant to my constitutional authority and consistent with sections 202(c) and (e) of the The District of Columbia Financial Management and Responsibility Assistance Act of 1995 and section 446 of The District of Columbia Self-Governmental Reorganization Act as amended in 1989, I am transmitting the District of Columbia's Fiscal Year 2003 Budget Request Act.

The proposed FY 2003 Budget Request Act reflects the major programmatic objectives of the Mayor and the Council of the District of Columbia. For FY 2003, the District estimates total revenue and expenditures of $5.7 billion.

GEORGE W. BUSH.

THE WHITE HOUSE, July 11, 2002.

REMEMBERING OUR VETERANS THROUGH SERVICE ORGANIZATIONS

(Mr. GEKAS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. GEKAS. Mr. Speaker, 1941 was a banner year for American baseball and baseball in the American League, as it were. In that year Joe DiMaggio hit in 56 games straight, and Ted Williams batted 406. These are not the important historical facts, although they are great for those of us who follow baseball, but both of them did something extraordinary. Joe DiMaggio, very soon after that wonderful streak, entered the United States Army and served until 1946 as a noncommissioned officer in the United States Army. Ted Williams went into the Air Force, or Army, and served the balance of the war in his branch of the service.

Then dramatically twice after that, Ted Williams reported back for duty and served in the Korean conflict. These are the great Americans that we remember and we will continue to remember through the service organizations which we will discuss a little bit later.

CORPORATE GREED

(Mr. BROWN of Ohio asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. BROWN of Ohio. Mr. Speaker, this morning in Birmingham, President Bush gave another speech aimed at restoring investor confidence at the same time the country's equity markets were well on their way to a sixth day of losses. Why is that?

Could it be because so many administration officials in the Bush White House are themselves former corporate CEOs, lawyers, or accountants who lack the moral authority or the will to change corporate practices, or even to enforce current law? Or could it be because in the middle of the current financial crisis, the President and the Vice President have been forced to answer questions about their own ethics and business practices as oil company CEOs? Or could it be, because despite his rhetorical calls for corporate America to clean up its act, the President continues to oppose real reform on Capitol Hill?

Maybe, Mr. Speaker, with the recent spate of corporate collapses, the American people have begun to wonder whether running the company like a corporation, as the President and Vice President have promised, is all that good an idea.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair announces that he will postpone further proceedings today on each motion to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote is objected to under clause 6 of rule XX.

Any record votes on motions to suspend the rules ordered prior to 6:30 p.m. will be taken today. Record votes on remaining motions to suspend the rules will be taken tomorrow.

CYBER SECURITY ENHANCEMENT ACT OF 2002

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3482) to provide greater cybersecurity, as amended.

The Clerk read as follows:

H.R. 3482

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Security Enhancement Act of 2002''.

TITLE I—COMPUTER CRIME

SEC. 101. AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES.

(a) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(b) REQUIREMENTS.—In carrying out this section, the Sentencing Commission shall—

(1) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in subsection (a), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(2) consider the following factors and the extent to which the guidelines may or may not account for them—

(A) the potential and actual loss resulting from the offense;

(B) the level of sophistication and planning involved in the offense;

(C) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(D) whether the defendant acted with malicious intent to cause harm in committing the offense;

(E) the extent to which the offense violated the privacy rights of individuals harmed;

(F) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(G) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(H) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(3) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(4) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(5) make any necessary conforming changes to the sentencing guidelines; and

(6) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

SEC. 101A. STUDY AND REPORT ON COMPUTER CRIMES.

Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this Act and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

SEC. 102. EMERGENCY DISCLOSURE EXCEPTION.

(a) IN GENERAL.—Section 2702(b) of title 18, United States Code, is amended—

(1) by striking ''or'' at the end of paragraph (5);

(2) by striking subparagraph (C) of paragraph (6);

(3) in paragraph (6), by inserting ''or'' at the end of subparagraph (A); and

(4) by inserting after paragraph (6) the following:

''(7) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.''.

(b) REPORTING OF DISCLOSURES.—A government entity that receives a disclosure under this section shall file, no later than 90 days after such disclosure, a report to the Attorney General stating the subparagraph under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The

Attorney General shall publish all such reports into a single report to be submitted to Congress one year after enactment of the bill.

SEC. 103. GOOD FAITH EXCEPTION.

Section 2520(d)(3) of title 18, United States Code, is amended by inserting ''or 2511(2)(i)'' after ''2511(3)''.

SEC. 104. INTERNET ADVERTISING OF ILLEGAL DEVICES.

Section 2512(1)(c) of title 18, United States Code, is amended—

(1) by inserting ''or disseminates by electronic means'' after ''or other publication''; and

(2) by inserting ''knowing the content of the advertisement and'' before ''knowing or having reason to know''.

SEC. 105. STRENGTHENING PENALTIES.

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

(1) by striking ''and'' at the end of paragraph (3);

(2) in each of subparagraphs (A) and (C) of paragraph (4), by inserting ''except as provided in paragraph (5),'' before ''a fine under this title'';

(3) by striking the period at the end of paragraph (4)(C) and inserting ''; and''; and

(4) by adding at the end the following:

''(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

''(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.''.

SEC. 106. PROVIDER ASSISTANCE.

(a) SECTION 2703.—Section 2703(e) of title 18, United States Code, is amended by inserting '', statutory authorization'' after ''subpoena''.

(b) SECTION 2511.—Section 2511(2)(a)(ii) of title 18, United States Code, is amended by inserting '', statutory authorization,'' after ''court order'' the last place it appears.

SEC. 107. EMERGENCIES.

Section 3125(a)(1) of title 18, United States Code, is amended—

(1) by striking ''or'' at the end of subparagraph (A);

(2) by striking the comma at the end of subparagraph (B) and inserting a semicolon; and

(3) by adding at the end the following:

''(C) an immediate threat to a national security interest; or

''(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;''.

SEC. 108. PROTECTING PRIVACY.

(a) SECTION 2511.—Section 2511(4) of title 18, United States Code, is amended—

(1) by striking paragraph (b); and

(2) by redesignating paragraph (c) as paragraph (b).

(b) SECTION 2701.—Section 2701(b) of title 18, United States Code, is amended—

(1) in paragraph (1), by inserting '', or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State'' after ''commercial gain'';

(2) in paragraph (1)(A), by striking ''one year'' and inserting ''5 years'';

(3) in paragraph (1)(B), by striking ''two years'' and inserting ''10 years''; and

(4) so that paragraph (2) reads as follows:

''(2) in any other case—

''(A) a fine under this title or imprisonment for not more than one year or both, in the case of a first offense under this paragraph; and

''(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.''.

(c) PRESENCE OF OFFICER AT SERVICE AND EXECUTION OF WARRANTS FOR COMMUNICATIONS AND CUSTOMER RECORDS.—Section 3105 of title 18, United States Code, is amended by adding at the end the following: ''The presence of an officer is not required for service or execution of a search warrant directed to a provider of electronic communication service or remote computing service for records or other information pertaining to a subscriber to or customer of such service.''.

TITLE II—OFFICE OF SCIENCE AND TECHNOLOGY

SEC. 201. ESTABLISHMENT OF OFFICE; DIRECTOR.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this title referred to as the ''Office'').

(2) AUTHORITY.—The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be independent of the National Institute of Justice.

(b) DIRECTOR.—The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

SEC. 202. MISSION OF OFFICE; DUTIES.

(a) MISSION.—The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) DUTIES.—In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of the Federal Advisory Committee Act (5 U.S.C. App.)) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113). The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, and evaluation in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.

(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.

(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.

(12) To support research fellowships in support of its mission.

(13) To serve as a clearinghouse for information on law enforcement technologies.

(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.

(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.

(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

(c) COMPETITION REQUIRED.—Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis.

(d) INFORMATION FROM FEDERAL AGENCIES.—Federal agencies shall, upon request from the Office and in accordance with Federal law, provide the Office with any data, reports, or other information requested, unless compliance with such request is otherwise prohibited by law.

(e) PUBLICATIONS.—Decisions concerning publications issued by the Office shall rest solely with the Director of the Office.

(f) TRANSFER OF FUNDS.—The Office may transfer funds to other Federal agencies or provide funding to non-Federal entities through grants, cooperative agreements, or contracts to carry out its duties under this section.

(g) ANNUAL REPORT.—The Director of the Office shall include with the budget justification materials submitted to Congress in support of the Department of Justice budget for each fiscal year (as submitted

with the budget of the President under section 1105(a) of title 31, United States Code) a report on the activities of the Office. Each such report shall include the following:

(1) For the period of 5 fiscal years beginning with the fiscal year for which the budget is submitted—

(A) the Director's assessment of the needs of Federal, State, and local law enforcement agencies for assistance with respect to law enforcement technology and other matters consistent with the mission of the Office; and

(B) a strategic plan for meeting such needs of such law enforcement agencies.

(2) For the fiscal year preceding the fiscal year for which such budget is submitted, a description of the activities carried out by the Office and an evaluation of the extent to which those activities successfully meet the needs assessed under paragraph (1)(A) in previous reports.

SEC. 203. DEFINITION OF LAW ENFORCEMENT TECHNOLOGY.

For the purposes of this title, the term ''law enforcement technology'' includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

SEC. 204. ABOLISHMENT OF OFFICE OF SCIENCE AND TECHNOLOGY OF NATIONAL INSTITUTE OF JUSTICE; TRANSFER OF FUNCTIONS.

(a) TRANSFERS FROM OFFICE WITHIN NIJ.—The Office of Science and Technology of the National Institute of Justice is hereby abolished, and all functions and activities performed immediately before the date of the enactment of this Act by the Office of Science and Technology of the National Institute of Justice are hereby transferred to the Office.

(b) AUTHORITY TO TRANSFER ADDITIONAL FUNCTIONS.—The Attorney General may transfer to the Office any other program or activity of the Department of Justice that the Attorney General, in consultation with the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, determines to be consistent with the mission of the Office.

(c) TRANSFER OF FUNDS.—

(1) IN GENERAL.—Any balance of appropriations that the Attorney General determines is available and needed to finance or discharge a function, power, or duty of the Office or a program or activity that is transferred to the Office shall be transferred to the Office and used for any purpose for which those appropriations were originally available. Balances of appropriations so transferred shall—

(A) be credited to any applicable appropriation account of the Office; or

(B) be credited to a new account that may be established on the books of the Department of the Treasury;

and shall be merged with the funds already credited to that account and accounted for as one fund.

(2) LIMITATIONS.—Balances of appropriations credited to an account under paragraph (1)(A) are subject only to such limitations as are specifically applicable to that account. Balances of appropriations credited to an account under paragraph (1)(B) are subject only to such limitations as are applicable to the appropriations from which they are transferred.

(d) TRANSFER OF PERSONNEL AND ASSETS.—With respect to any function, power, or duty, or any program or activity, that is transferred to the Office, those employees and assets of the element of the Department of Justice from which the transfer is made that the Attorney General determines are needed to perform that function, power, or duty, or for that program or activity, as the case may be, shall be transferred to the Office.

(e) REPORT ON IMPLEMENTATION.—Not later than 1 year after the date of the enactment of this Act, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the implementation of this title. The report shall—

(1) identify each transfer carried out pursuant to subsection (b);

(2) provide an accounting of the amounts and sources of funding available to the Office to carry out its mission under existing authorizations and appropriations, and set forth the future funding needs of the Office;

(3) include such other information and recommendations as the Attorney General considers appropriate.

SEC. 205. NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTERS.

(a) IN GENERAL.—The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as ''Centers'') and, to the extent necessary, establish new centers through a merit-based, competitive process.

(b) PURPOSE OF CENTERS.—The purpose of the Centers shall be to—

(1) support research and development of law enforcement technology;

(2) support the transfer and implementation of technology;

(3) assist in the development and dissemination of guidelines and technological standards; and

(4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

(c) ANNUAL MEETING.—Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

(d) REPORT.—Not later than 12 months after the date of the enactment of this Act, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

SEC. 206. COORDINATION WITH OTHER ENTITIES WITHIN DEPARTMENT OF JUSTICE.

Section 102 of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3712) is amended in subsection (a)(5) by inserting ''coordinate and'' before ''provide''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin (Mr. SENSENBRENNER) and the gentlewoman from Texas (Ms. JACKSON-LEE) each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin (Mr. SENSENBRENNER).

GENERAL LEAVE

Mr. SENSENBRENNER. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on H.R. 3482.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Wisconsin?

There was no objection.

Mr. SENSENBRENNER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, our society has become technologically dependent. Computers and related technologies have improved every aspect of our lives, our health care, our education, and our security. Unfortunately, this same technology has also facilitated terrorist and criminal activity alike. At the stroke of a key, someone can cause millions of dollars of damage to our economy as well as threaten our national security and the public's safety.

This threat is not new; but after the September 11 attacks, the risks are greater. Even prior to the attacks, the Committee on the Judiciary's Subcommittee on Crime, Terrorism, and Homeland Security was working on legislation to improve Federal law to protect the Nation from cybercrime and cyberterrorism.

Last summer, the subcommittee held three hearings on the growing threat of cybercrime and cyberterrorism. Those hearings highlighted the fact that cybercrime knows no borders or restraints and can substantially harm the American people and our economy.

The law enforcement officials and private industry representatives at the hearings agreed that better coordination, cooperation and information-sharing were needed as well as stronger penalties for cyberattacks.

The U.S.A. PATRIOT Act, which the Committee on the Judiciary adopted much of H.R. 2915, an earlier cybersecurity bill introduced by the gentleman from Texas (Chairman SMITH), and began to improve the Nation's cybersecurity, this bill, the Cyber Security Enhancement Act of 2002, continues that work.

The bill strengthens penalties to better reflect the seriousness of cyberattacks, assists State and local law enforcement through better grant management, accountability and dissemination of technical advice and information, helps protect the Nation's critical infrastructure, and enhances privacy protections.

On May 8, the Committee on the Judiciary reported this bill favorably by voice vote. The bill as introduced and reported out of committee contained an authorization for the National Infrastructure Protection Center within the Department of Justice.

Since that time, it appears that the center will be transferred out of the Department of Justice into the new Department of Homeland Security proposed in H.R. 5005. Accordingly, the committee has removed that authorization to be consistent with H.R. 5005 in this amended version of H.R. 3482. The bill also contains a few technical changes as well.

H.R. 3482, the Cyber Security Enhancement Act of 2002, is designed to increase the cybersecurity of our Nation against criminal and terrorist attacks. As one of the most technologically advanced nations in the world, we must deal with a new vulnerability, the interconnectedness of our Nation's economy and national security. I urge Members to support this bill.

Mr. Speaker, I reserve the balance of my time.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I yield myself such time as I may consume.

(Ms. JACKSON-LEE of Texas asked and was given permission to revise and extend her remarks.)

Ms. JACKSON-LEE of Texas. Mr. Speaker, I rise to join the gentleman from Wisconsin (Mr. SENSENBRENNER) in support of H.R. 3482, the Cyber Security Act of 2002. I support the concept of allowing internal service providers to give information to law enforcement officials when emergency threat of death or serious bodily injury exists.

In general, information held by an ISP is private information which is entitled to protection as such. In fact, we have worked very hard to ensure that the privacy of Internet users and providers have been secured. This is a new way that America provides its information and communication; and, therefore, we believe the privacy issues are extremely important.

□ 1415

Under current law, an ISP is authorized to release information to law enforcement officials when the ISP reasonably believes an immediate danger exists. For an ISP to reasonably believe an immediate danger exists, an assessment of relevant information must be made. However, if the FBI presents information which an ISP believes, if true, would present a threat of death or serious bodily injury, the ISP dispatcher on duty should not have to wake up the corporate general counsel to assess the information to determine if it can be reasonably believed, particularly as relates to saving lives. If there is time to do all that, there is time to go to a magistrate or judge and get a search warrant. Accordingly, I would support changing ''reasonably believed'' to ''believes in good faith'' as the bill does.

I appreciate the adjustments Subcommittee Chairman SMITH made to the bill to address concerns that we had with the bill and Ranking Member SCOTT had with the bill, including adding a reporting requirement for law enforcement officials to report on their use of the provision during the year following enactment so that we can see how it is being used. This is in keeping with the balance that I think is important in fighting terrorism and providing law enforcement officers with the tools that they need, as well as balancing the rights of Americans. It is one thing to use this emergency authority for genuine emergencies involving threats to life or safety. It is another thing to use it in a calculated manner to get around the regular requirement of obtaining a warrant from a detached magistrate or judge before being given access to private information. Since the subscriber may never know of the access by law enforcement to his or her private information, there will be no way to know if they are assessing information erroneously or improperly. With this particular requirement, providing this information in the year following, this will help determine that. With the reporting requirement, we should be able to assess whether this provision is being used as contemplated and not abused.

With this understanding of the bill, Mr. Speaker, I support it and urge my colleagues to vote for it.

Mr. Speaker, I rise to join Chairman SENSENBRENNER in support of H.R. 3482, the Cyber Security Act of 2001.

I support the concept of allowing Internet Service Providers (ISP) to give information to law enforcement officials when an emergency threat of death or serious bodily injury exists. In general, information held by an ISP in private information which is entitled to protection as such. Under current law, an ISP is authorized to release information to law enforcement officials when the ISP ''reasonably believes'' an immediate danger exists. For an ISP to ''reasonably believe'' an immediate danger exists, an assessment of relevant information must be made. However, if the FBI presents information which an ISP believes, if true, would present a threat of death or serious bodily injury, the ISP dispatcher on duty shouldn't have to wake up the corporate general counsel to assess the information to determine if it can be reasonably believed. If there is time to do all that, there is time to go to a magistrate or judge and get a search warrant. Accordingly, I support changing ''reasonably believes'' to ''believes in good faith'', as the bill does.

I appreciate the adjustments Subcommittee Chairman SMITH made to the bill to address concerns I had with the bill, including adding a reporting requirement for law enforcement officials to report on their use of the provision during the year following enactment, so that we can see how it is being used. It is one thing to use this emergency authority for genuine emergencies involving threats to life or safety, it is another thing to use it in a calculated manner to get around the regular requirement of obtaining a warrant from a detached magistrate or judge before being given access to private information. Since the subscriber may never know of the access by law enforcement to his or her private information, there will be no way to know if they are accessing information erroneously or improperly. With the reporting requirement, we should be able to assess whether this provision is being used as contemplated, and not abused.

With this understanding of the bill, Mr. Speaker, I support it and urge my colleagues to vote for it.

Mr. Speaker, I reserve the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield 4 minutes to the gentleman from Texas (Mr. SMITH), the subcommittee chairman.

Mr. SMITH of Texas. Mr. Speaker, I thank the chairman of the Committee on the Judiciary for yielding me this time.

Mr. Speaker, many people think of cybercrime simply as a form of vandalism involving hacking or planting viruses. Cybercrime is much more than this. It can devastate our businesses, economy and national infrastructure. Cybercrime also includes child pornography, which terrorizes our children and our families. Criminals use computer technology to steal life savings and the identities of unsuspecting individuals. These attacks threaten the lives and the livelihoods of many innocent victims.

Mr. Speaker, a crime is still a crime, whether it occurs on the Internet or on the street. We are in a war against terrorism. According to a recent newspaper article, ''Unsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed.''

The article stated, ''Most significantly, perhaps, U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport and communication grids.''

Cybercrimes and cybercriminals know no borders. As long as there is technology, cybercrime will exist. We must improve our Nation's cybersecurity and strengthen our criminal laws to prevent, deter and respond to such attacks.

This legislation, H.R. 3482, the Cyber Security Enhancement Act of 2002, increases penalties to better reflect the seriousness of cybercrime, enhances Federal, State and local law enforcement efforts through better coordination, and assists State and local law enforcement officials through better grant management, accountability and dissemination of technical advice and information. The Information Technology Association of America stated that the bill is important for strengthening guidelines on sentencing people who are convicted of cybercrimes. The Information Technology Industry Council concluded that the bill will remove obstacles to information-sharing between the public and private sectors to strengthen Internet security.

Mr. Speaker, we must protect our Nation and our economy from the growing threat of cyberattacks. Penalties and law enforcement capabilities must be able to prevent and deter cybercriminals. Until we secure our cyberinfrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy or endanger lives. A mouse can be just as dangerous as a bullet or a bomb. That is why I urge my colleagues to support this legislation.

Mr. SENSENBRENNER. Mr. Speaker, I yield such time as he may consume to the gentleman from New York (Mr. BOEHLERT), the chairman of the Committee on Science.

Mr. BOEHLERT. I thank the gentleman for yielding me this time.

Mr. Speaker, I rise in strong supports of H.R. 3482, the Cyber Security Enhancement Act of 2002. I want to thank the gentleman from Texas (Mr. SMITH), the Subcommittee on Crime, Terrorism and Homeland Security chairman, for his excellent work in bringing this bipartisan bill to the floor. I also want to thank the gentleman from Wisconsin (Mr. SENSENBRENNER), Judiciary chairman, former chairman of the Committee on Science, where he received

his best training. From his years of service on the Committee on Science, the gentleman from Wisconsin understands that research and development are critical weapons in the war on terrorism as well as our fight against all forms of crime. We know that the next war, the current war, the ongoing war, is going to be won as much in the laboratory as on the battlefield.

Mr. Speaker, title I of the legislation enhances penalties for cybercrime and allows for better cooperation between law enforcement and the private sector to investigate cybercrime. This is critical. However, in the interest of time, I will limit my comments to title II of the bill before the House today.

Title II establishes an Office of Science and Technology within the Office of Justice Programs at the Justice Department. It is a needed step forward in our fight against all forms of crime and terrorism. I have said repeatedly, the war on terrorism, like the Cold War, will be won in the laboratory as much as on the battlefield. That means that, as in the Cold War, we must properly organize our government to put the most into and get the most out of our academic, government and industry laboratories. Criminal use of technology, specifically information technology, is now commonplace. We rely on computers, the Internet, cell phones and pagers every day. But so, too, do the criminals and terrorists.

Increasingly criminals are becoming more and more sophisticated. Online fraud, identity theft, child pornography, computer intrusions, hacking and introduction of viruses are all on the rise. Unfortunately, U.S. law enforcement is often ill-equipped to counter this criminal high tech trend. It is particularly true for State and local law enforcement that often lack the resources, training and expertise to effectively use advanced information technology to stop crime. Currently the Justice Department does support the development of new technologies, mostly through the National Institute of Justice, to serve the needs of law enforcement and corrections agencies, but the effort as it stands today is unfocused and limited.

That is why I have sought for over 3 years to establish an office for science and technology within the Department of Justice with the mission of improving the technical capabilities of law enforcement at all levels. The bill before us today would do just that. Let me also note that this bill would not create a new bureaucracy. In fact, the Congressional Budget Office has scored this bill as revenue-neutral. Rather, the bill would transfer existing assets within the Justice Department to give the agency an improved science and technology capability to better respond to threats posed by technically savvy criminals and terrorists. This is a commonsense proposition. U.S. law enforcement agencies traditionally do not have research and development capabilities like those found in the military. Rather than creating a new R&D infrastructure for law enforcement, we must find ways to help law enforcement gain access to the scientific expertise found in our colleges and universities as well as our defense and national laboratories.

H.R. 3482 does this by explicitly authorizing DOJ's existing network of regional technology assistance centers, the National Law Enforcement and Corrections Technology Centers. These centers are able to leverage existing defense capabilities in sensitive areas such as information security, chemical, biological and nuclear security to provide Federal, State and local law enforcement access to the best technologies available to meet these emerging threats.

In my home district, one such center is leading the Nation in the fight against cybercrime and all forms of crime. This is the National Law Enforcement and Corrections Technology Center, Northeast Region, located at the Air Force Research Laboratory Information Directorate at Rome, New York. A prominent example of the center's work was the establishment of the highly successful Utica Arson Strike Force in 1997. In less than a year, the city went from worst to first in the Nation in the rate of arson convictions. Leveraging the high tech expertise of the Air Force research laboratory, the center was able to create affordable technology tools for the Utica task force's use.

While the track record of the center and others around the Nation is impressive, the amount of resources available for technical assistance is meager. The entire center system, as well as the science and technology function within the Department of Justice, needs a clear congressional mandate and an adequate budget. This bill would bring needed focus to R&D in support of law enforcement and establish the Office of Science and Technology as a key liaison between DOJ and other Federal research agencies.

Mr. Speaker, the Committee on Science recently heard testimony from a distinguished panel of the National Academy of Sciences about the need for greater science and technology investment to combat terrorism. For this reason, the Committee on Science unanimously approved the creation of an under secretary for research and development in the proposed Homeland Security Department. The bill before us today is consistent with this vision. As we move forward in this process, I hope to forge a close working partnership between DOJ's Office of Science and Technology and the new Homeland Security Department.

I look forward to working with Chairman SENSENBRENNER, Chairman SMITH and all members of the Committee on the Judiciary to ensure appropriate coordination of effort to help combat terrorism and to ensure that more and more State and local first responders have access to first-rate scientific and technological expertise.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I yield myself such time as I may consume. I rise to support this legislation. I just want to make note that this legislation has provided a reporting requirement placed in the bill to help address the concerns, making sure that the legislation is used properly. I would have liked to have added additional safeguards dealing with the unreasonable search and seizure, but I believe that the reporting requirement will go a long ways to addressing that concern, and I would ask my colleagues to support this legislation.

Mr. GILMAN. Mr. Speaker, I rise today in strong support of H.R. 3482, the Cyber Security Enhancement Act of 2002.

This resolution achieves several goals. The act will serve as a national focal point for science and technology and it will also aid in the development and dissemination of cyber law enforcement and technology.

Moreover, it will make technical assistance available to Federal, State, and local law enforcement agencies which is increasingly critical for our national security and infrastructure.

Crimes of fraud in computers with protected information or computers used by the Federal Government are addressed in the legislation.

A program will be established and maintained to certify, validate, and mark, or otherwise recognize law enforcement technology products that conform to standards set by the National Infrastructure Protection Center.

The National Infrastructure Protection Center will operate for regional national law enforcement and corrections technology centers and, to the extent necessary, establish additional centers through a competitive process.

This bill further provides that law enforcement agencies utilize and establish forensic technology, and technologies that support the judicial process.

The use of these forensic tools will assist State and local law enforcement agencies in combating cybercrime. In addition, penalties will increase for violations where the offender knowingly causes death or serious bodily injury.

Mr. Speaker, I urge this body to support this measure as it addresses the growing and increasingly visible problem of cybercrime.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I yield back the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. CULBERSON). The question is on the motion offered by the gentleman from Wisconsin (Mr. SENSENBRENNER) that the House suspend the rules and pass the bill, H.R. 3482, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

Ms. JACKSON-LEE of Texas. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.