AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

107TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 107–497

CYBER SECURITY ENHANCEMENT ACT OF 2002

JUNE 11, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 3482]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 3482) to provide greater cybersecurity, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
The Amendment	1
Purpose and Summary	6
Background and Need for the Legislation	7
Hearings	8
Committee Consideration	8
Vote of the Committee	9
Committee Oversight Findings	9
Performance Goals and Objectives	9
New Budget Authority and Tax Expenditures	9
Congressional Budget Office Cost Estimate	9
Constitutional Authority Statement	11
Section-by-Section Analysis and Discussion	11
Agency Views	21
Changes in Existing Law Made by the Bill, as Reported	27
Markup Transcript	32

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

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

99–006

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. NATIONAL INFRASTRUCTURE PROTECTION CENTER.

(a) IN GENERAL.—The Attorney General shall establish and maintain a National Infrastructure Protection Center (hereinafter in this section referred to as the "Center") to serve as a national focal point for threat assessment, warning, investigation, and response to attacks on the Nation's critical infrastructure for both physical and cyber sources.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for fiscal year 2003 to carry out this section, $125,000,000.

SEC. 105. 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. 106. 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. 107. 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. 108. 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. 109. 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 warrant under section 2703 when the provider of electronic communications service or remote computing service produces the information required in the warrant.".

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 used by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), which may, in the discretion of the Office, allow for supplier 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".

PURPOSE AND SUMMARY

H.R. 3482, the "Cyber Security Enhancement Act of 2002," would increase penalties for cybercrimes to better reflect the seriousness of the crime; enhance law enforcement efforts through better coordination; provide the authority and resources for the National Infrastructure Protection Center to serve as a national focal point for

threat assessment, warning, investigation, and response to attacks on the nation's critical infrastructure from both physical and cyber sources; and make the Office of Science and Technology an independent office to serve as the national focal point for law enforcement science and technology and to assist in the development and dissemination of law enforcement technology, and to make technical assistance available to Federal, State, and local law enforcement agencies.

BACKGROUND AND NEED FOR THE LEGISLATION

Since the beginning of the 107th Congress, the Subcommittee on Crime, Terrorism, and Homeland Security has examined the need for legislation to update and improve Federal law to protect the nation from cyber-crime and -terrorism.

On May 24, 2001, the Subcommittee heard from three State and local officials on law enforcement efforts and needs to fight cybercrime, expressing views from the police, the prosecutors and the State governments. The witnesses were Michael T. McCaul, the Texas Deputy Attorney General for Criminal Justice; the Honorable Joseph I. Cassilly, the State's Attorney for Harford County, Maryland and Chairman of the Cyber Crime Committee for the National District Attorneys Association; and Ronald R. Stevens, the Senior Investigator for the Bureau of Criminal Investigation for the New York State Police, Computer Crime Unit. All three testified with regard to the need for better resources, training, standards, and equipment.

On June 12, 2001, officials from three Federal agencies testified before the Subcommittee. The witnesses were Michael Chertoff, the Assistant Attorney General of the Criminal Division for the Department of Justice; Thomas T. Kubic, the Deputy Assistant Director of the Criminal Investigative Division for the Federal Bureau of Investigation; and James A. Savage, Jr., the Deputy Special Agent in Charge of the Financial Crimes Division for United States Secret Service. These three witnesses agreed that Federal laws regarding the processes and procedures to investigate and prosecute cybercrime were outdated in certain areas.

Alan Davidson, Associate Director at the Center for Democracy and Technology (CDT), a Washington, DC, non-profit group interested in civil liberties and human rights on the Internet and other new digital media, also testified. He urged the Subcommittee to consider privacy issues when drafting new legislation and updating the law. At a February 12, 2002 legislative hearing on H.R. 3482, the "Cyber Security Enhancement Act of 2002," Mr. Davidson testified that the "[Center for Democracy and Technology (CDT)] commends this Committee for holding this hearing, and for the relatively measured approach taken in H.R. 3482. We agree that computer crime and security is a serious problem that requires serious Government response."

On June 14, 2001, representatives from the business community testified about the problems they face with cybercrime. The hearing focused on the efforts and concerns of private industry with regard to this issue. The witnesses agreed that sharing information was key to successfully addressing and preventing cybercrime. Additionally, the witnesses urged Congress to examine stricter penalties for cybercrime.

The three hearings highlighted the growing threat of cybercrime and cyberterrorism against our citizens and our nation and the definitive need for legislation. Criminals use computers and other types of technology to target the income and well-being of American citizens, the nation's economy, America's national security, and our critical infrastructure.

On September 20, 2001, H.R. 2915, "the Public Safety and Cyber Security Enhancement Act of 2002" was introduced to address the concerns brought forth in the hearings. Most of H.R. 2915 was adopted as part of the USA PATRIOT Act [1], the anti-terrorism bill, that was enacted in October 26, 2001. There remained some additional issues that were not addressed.

H.R. 3482, "the Cyber Security Enhancement Act of 2002," responds to the previous hearings and ongoing discussions with law enforcement, industry, and academia representatives and the need to address issues not covered in the USA PATRIOT Act.

While technology has improved the standard of living for the United States and her citizens, it has also assisted criminals and terrorists with their nefarious activities. Terrorists and high-tech vandals use computers and other technology to terrorize and harass businesses, private citizens and the Government, which costs the taxpayers millions. For example, hackers are invading the privacy of our citizens' homes to program personal computers into "zombie computers." These zombie computers are then used for the denial-of-service attacks that bombard a target site with nonsense data. In February 2000, a denial-of-service attack on Yahoo and other companies cost millions of dollars. These types of attacks not only threaten our economy, but also our public safety. An attack on an emergency service network could prevent prompt responses to people in life threatening situations, causing injury or death.

The protection of our national security, critical infrastructure and economic base is essential. The terrorist attacks on September 11th severely affected our economy and demonstrated a need to evaluate and improve our security. A terrorist or criminal cyber attack could further harm our economy and critical infrastructure. It is imperative that the penalties and law enforcement capabilities are adequate to prevent and deter such attacks.

HEARINGS

The Committee's Subcommittee on Crime held 1 day of hearings on H.R. 3482 on February 12, 2002. Testimony was received from four witnesses: John G. Malcolm, Deputy Assistant Attorney General, Criminal Division of the Department of Justice; Susan Kelley Koeppen, Corporate Attorney, Microsoft Corporation; Clint Smith, Vice President and Chief Network Counsel of WorldCom; and Alan Davidson, Staff Counsel, Center for Democracy and Technology.

COMMITTEE CONSIDERATION

On February 26, 2002, the Subcommittee on Crime met in open session and ordered favorably reported the bill H.R. 3482, as amended, by a voice vote, a quorum being present. On May 1, 2002, the Committee met in open session and ordered favorably reported

[1] Pub. L No. 107–56.

the bill H.R. 3482, with an amendment in the nature of a substitute, by voice vote, a quorum being present.

VOTE OF THE COMMITTEE

There were no recorded votes on H.R. 3482.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

PERFORMANCE GOALS AND OBJECTIVES

The bill is intended to improve the ability of Federal, State and local law enforcement efforts to deter, prevent and resolve cyber attacks carried out by terrorists and other criminals. The bill will implement accountability in the management of grants for technology investment at the State and local levels through assessments and better Federal grant management. Additionally, the bill will improve the protection of the nation's critical infrastructure from cyber and physical attacks.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of House rule XII is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3482, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 22, 2002.

Hon. F. JAMES SENSENBRENNER, Jr., *Chairman,*
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3482, the Cyber Security Enhancement Act of 2002.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226–2860.

Sincerely,

DAN L. CRIPPEN, *Director.*

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 3482—Cyber Security Enhancement Act of 2002.

SUMMARY

H.R. 3482 would authorize the appropriation of $125 million for fiscal year 2003 for the National Infrastructure Protection Center (NIPC) in the Department of Justice. The bill also would establish new federal crimes and would increase penalties for unauthorized use of computers and related offenses.

CBO estimates that implementing H.R. 3482 would cost $125 million over the 2003–2004 period, subject to appropriation of the authorized amount. Enacting the bill also would affect direct spending and receipts, but CBO estimates that any such effects would not be significant. Because the bill would affect direct spending and receipts, pay-as-you-go procedures would apply.

H.R. 3482 would impose reporting requirements on State and local government agencies that receive certain disclosures from providers of electronic communication services. Such a requirement would constitute an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that the cost of complying with these new reporting requirements would not likely be significant, and would not exceed the threshold established in UMRA ($58 million in 2002, adjusted annually for inflation). Overall, the bill would benefit State, local, and tribal governments by providing technological assistance and training materials to State and local law enforcement agencies. H.R. 3482 contains no new private-sector mandates as defined in UMRA.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 3482 is shown in the following table. CBO assumes that the amounts authorized for the NIPC will be appropriated by the start of fiscal year 2003. We expect that outlays will occur somewhat more slowly than the historical rate of spending for this program because of the increase in funding compared to the 2002 level. The costs of this legislation fall within budget function 750 (administration of justice).

By Fiscal Year, in Millions of Dollars

	2002	2003	2004	2005	2006	2007
SPENDING SUBJECT TO APPROPRIATION						
Spending for NIPC Under Current Law						
Budget Authority [1]	90	0	0	0	0	0
Estimated Outlays	75	25	0	0	0	0
Proposed Changes						
Authorization Level	0	125	0	0	0	0
Estimated Outlays	0	88	38	0	0	0
Spending for NIPC Under H.R. 3482						
Authorization Level	90	125	0	0	0	0
Estimated Outlays	75	113	38	0	0	0

1. The 2002 level is the amount appropriated for that year for the National Infrastructure Protection Center.

Enacting H.R. 3482 could increase collections of criminal fines for unauthorized use of computers and other offenses. CBO estimates that any additional collections would not be significant. Criminal

fines are recorded as receipts and deposited in the Crime Victims Fund, then later spent.

PAY-AS-YOU-GO CONSIDERATIONS

The Balanced Budget and Emergency Deficit Control Act specifies pay-as-you-go procedures for legislation affecting direct spending and receipts. These procedures would apply to H.R. 3482 because it would affect both direct spending and receipts, but CBO estimates that the annual amount of such changes would not be significant.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 3482 would impose reporting requirements on State and local government agencies that receive certain disclosures from providers of electronic communication services. Such a requirement would constitute an intergovernmental mandate as defined in UMRA. CBO estimates that the cost of complying with these new reporting requirements would not likely be significant, and would not exceed the threshold established in UMRA ($58 million in 2002, adjusted annually for inflation). Overall, the bill would benefit State, local, and tribal governments by providing technological assistance and training materials to State and local law enforcement agencies.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 3482 contains no new private-sector mandates as defined in UMRA.

ESTIMATE PREPARED BY:

Federal Costs: Mark Grabowicz (226–2860)
Impact on State, Local, and Tribal Governments: Angela Seitz (225–3220)
Impact on the Private Sector: Paige Piper/Bach (226–2960)

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article I, section 8, of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

Sec. 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.

This section would direct the United States Sentencing Commission to review, and if appropriate amend, the Federal sentencing guidelines to provide a wider range of criteria for sentencing of those convicted for cybercrimes under 18 U.S.C. § 1030. The Committee is concerned that the sentencing guidelines do not adequately account for the serious nature of computer crimes. Computer crimes can cost businesses millions of dollars, can harm the nation's economy, threaten public safety, and violate the privacy of individuals.

Recognizing the growing threats posed by cybercrime, Congress, in the USA PATRIOT Act,[2] increased maximum penalties for certain violations of 18 U.S.C. § 1030 that can threaten lives as well as national security. Additionally, the USA PATRIOT Act added three new violations under section 1030 where the offense involved an attack on computers used by the Government in furtherance of national defense, national security, or the administration of justice. This section of the bill reflects those changes.

This section of the bill also reflects the enhanced penalties for cybercrime under H.R. 3482. In section 106, the bill enhances the maximum penalty for cybercrimes where an offender of 18 U.S.C. § 1030 knowingly or recklessly causes or attempts to cause death or serious bodily injury through a cyber attack. This section also covers the grave threat that cyber attacks pose to critical infrastructures.

The Committee believes that the United States Sentencing Commission must review the guidelines to ensure that they appropriately reflect the grievous nature of cyber attacks. The Committee believes that these new guidelines will allows judges to better account for the seriousness of a computer crime. Judges will be able to consider, among other things, the level of sophistication of the offense, whether the defendant acted with malicious intent to cause harm in committing the offense, and the extent to which the privacy rights of the victims of the crime were violated.

This section also requires the U.S. Sentencing Commission to submit by May 1, 2003, to Congress a brief report that explains any actions taken by the Sentencing Commission in response to this act.

Sec. 102. Emergency Disclosure Exception.

Under current law, communication providers are prohibited from disclosing electronic stored communications unless the disclosure is under a specified exception. One of those exceptions, 18 U.S.C. § 2702(b)(6)(C), provides that a communication service provider may disclose a communication to a law enforcement agency if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay. Communication providers expressed concern to the Committee that the standard

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Pub. L. No. 107–56.

was too difficult for them to meet and that, as a result, providers may not disclose information relating emergencies, such as a biological terrorist attack, to the appropriate Government officials.

This section would amend the current law to allow communications providers to disclose communications to a Federal, State or local government entity in emergency situations. The provider could only disclose communications that relate to the emergency if the provider, in good faith, believes that an emergency exists and that the emergency involves a danger of death or serious physical injury which requires disclosure without delay.

Specifically, this section would make three changes to current law to enhance cooperation with law enforcement and communications providers. First, it would change the legal standard for providers to determine whether there is an emergency from "reasonable" to "good faith." Second it would remove the requirement that a provider determine what is or is not an immediate danger. Third, the provision would allow the provider to disclose the information to any Government entity, such as the Centers Disease Control (CDC), as well as to law enforcement.

Based upon the testimony presented to the Subcommittee on Crime at the February 12, 2002 hearing, the Committee believes that changing the standard for providers from reasonable to good faith is an appropriate and a necessary change. As Susan Koeppen testified, providers are concerned that "communications providers or Internet Service Providers may be unnecessarily constrained in making decisions in good faith to disclose information in an emergency situation involving the danger of death or serious physical injury which requires immediate disclosure of that information." She went on to testify that section 102 made "several improvements to existing law that will enable such providers to make decisions promptly and without hesitation in emergency situations."

The Committee finds that certain emergencies may make it more appropriate for a provider to call the CDC or a hospital instead of, or in addition to, law enforcement, and thus the notification restriction should not be limited to law enforcement.

Additionally, the word "immediate" is not needed. The language of the bill requires that the provider, in good faith, believes (1) that there is an emergency, (2) that emergency involves danger of death or serious physical injury, and (3) that the emergency requires disclosure of the communications without delay. The American Heritage College dictionary defines "emergency" as "a serious situation or occurrence that happens unexpectedly and demands immediate action."

Furthermore, the provider must have a good faith belief that the information should be disclosed without delay.

Accordingly, the Committee believes Congress should not add an additional "immediate" requirement that makes the provider determine whether or not the danger itself is immediate. For example, if someone plans to bomb an elementary school next week, then the communications provider should be able to disclose that information and not have to guess whether an action which is to occur a week later constitutes "an immediate" danger or not. In such a case, law enforcement may need all the time it can get to locate the perpetrator and prevent the crime. Another example is where an individual sends an e-mail to another person describing an up-

coming terrorist attack he or she is planning, but does not put a date on the attack. A terrorist attack would clearly constitute an emergency that threatens life or limb, but the timing of the attack may not be evident. The attack could be planned for tomorrow or for a year from now. It is clear that there is a danger, but the immediacy of that danger is unclear.

Accordingly, this section changes current law to reflect the fact that if a provider, in good faith, believes there is an emergency, the provider should not be held liable. The Committee would note that section 102 of this bill does not change the standard or lower the standard for law enforcement behavior. This section, instead, requires that a communications provider must have a "good faith" belief that there is an emergency involving danger of death or serious physical injury to any person that requires disclosure without delay. This section is aimed at protecting providers who in good faith attempt to assist law enforcement with an emergency situation.

This section *does not* reduce the standard under which law enforcement must act. If police abuse that standard, there are appropriate consequences. The courts have applied a judicially created exclusionary rule for years. As the Supreme Court stated the rule exists as a "judicially created remedy designed to safeguard Fourth amendment rights generally through its deterrent effect. . . ."[3]

Any criminal evidence that is secured, directly or indirectly, in violation of the Fourth amendment, may not be admitted against a defendant in a criminal proceeding. A police officer who makes a false claim to a communications provider that there is an emergency that authorizes the disclosure of information under section 102 of the Cyber Security Enhancement Act has conducted an illegal search and seizure. The police officer must have a reasonable belief to make such a claim and if she or he does not, the evidence would be subject to the existing judicially created exclusionary rule.

Finally, this section would require Government officials to report quarterly to the Attorney General for the first year after enactment of the bill. At the end of that year, the Attorney General would send a report on the quarterly reports to Congress. This is a one time reporting requirement for the Attorney General.

Sec. 103. Good Faith Exception.

This section would update the "good faith reliance" defense in 18 U.S.C. § 2520(d) so that the new computer trespasser law[4] created in section 217 of the USA PATRIOT Act is also covered. Current law provides that a communications provider that relies in good faith on a court order or other listed authorization has a complete defense against civil or criminal action brought under this chapter or any other law. It appears that the current defense, as written,

---

[3] *United States* v. *Leon*, 468 U.S. 897, 906 (1984), quoting *United States* v. *Calandra*, 414 U.S. 338,348 (1974), quoted with approval in *Illinois* v. *Krull*, 480 340, 347 (1987); see also *Terry* v. *Ohio*, 392 U.S. 1, 12–4 (1968); *United States* v. *Janis*, 428 U.S. 433, 446 (1976).

[4] Prior to the enactment of the USA PATRIOT Act, victims of a computer trespasser attack were not able to authorize law enforcement to intercept the trespassers communications. Rather law enforcement would have had to go to get a court order to help the owners of systems providing communication services protect their own systems. The USA PATRIOT Act amended the law to clarify that law enforcement may intercept such communications when authorized by the victims.

would not cover a provider acting in good faith under the new computer trespasser law to assist law enforcement.

This section clarifies that communications providers, who assist law enforcement officials under the new computer trespasser are covered. This language was included in the House version of the PATRIOT Act[5] that was reported unanimously out of Committee. The final version of the USA PATRIOT Act, however, adopted the Senate language that did not include this provision.

This section simply clarifies that communications providers assisting law-enforcement under this section will continue to be covered by the good faith reliance defense under 18 U.S.C. § 2520.

Sec. 104. National Infrastructure Protection Center.

This section authorizes the Attorney General to establish and maintain a National Infrastructure Protection Center (NIPC) to serve as a national focal point for threat assessment, warning, investigation, and response to attacks on the nation's critical infrastructure from both physical and cyber sources. This section authorizes the appropriation of $125,000,000 for fiscal year 2003.

The Committee believes that information sharing is a key to protecting the security of the nation. The NIPC facilitates information sharing to protect the critical infrastructure of the nation. It was created in 1998, but it was not authorized. In addition to working with Federal, State and local Government officials, NIPC works with private sector infrastructure owners and operators.

The Committee believes that the war on terrorism demands additional efforts to protect the nation's critical infrastructure. By authorizing NIPC, the Congress demonstrates its support for this important task.

Sec. 105. Internet Advertising of Illegal Devices.

Section 105 was included to address a statutory loophole that allows for the distribution of advertisements of illegal interception devices through contemporary means of communication. This section would amend 18 U.S.C. § 2512(1)(c) to make the language technology neutral and close the existing loophole to further protect privacy. Under current law, 18 U.S.C. § 2512(1)(c) prohibits the advertisement of illegal interception devices in any magazine, newspaper, handbill, or other publication. The current law, however, does not mention advertising such devices on the Internet. This section would correct that loophole and ensure consistent treatment among advertising mediums by amending 18 U.S.C. § 2512(1)(c) to include the advertisements disseminated by electronic means.

Sec. 106. Increased Penalty.

This section amends 18 U.S.C. § 1030(c) to allow for criminal penalties to be increased if the offender knowingly or recklessly causes or attempts to cause death or serious bodily injury through a cyber attack. When a terrorist or other criminal attacks a computer system that, for instance, controls the 9–1–1 telephone systems, and causes a death or deaths, the current 10-year prison term may not be enough. This section provides the flexibility for a

[5] Provide Appropriate Tools Required to Intercept and Obstruct Terrorism, H.R. 2975, H. Rep. No. 107–236, Part 1.

more severe punishment when the computer crime is severe. The Committee believes that cyber attacks can pose a serious threat to life and limb and that the penalties should reflect that threat.

Sec. 107. Provider Assistance.

This section would ensure that providers of communications remain covered under 18 U.S.C. § 2703(e), a "no cause of action provision," which protects providers from law suits when they legally assist law enforcement with an investigation under the new emergency disclosure exception created in section 212 of the USA PATRIOT Act. Under current law, there is a "no cause of action [protection] against providers disclosing information . . . in accordance with the terms of a court order, warrant, subpoena, or certification under [chapter 121]." Section 107 would add information disclosed under "statutory authorization," to cover providers that contact authorities in emergency situations. This language was previously included in the House version of the PATRIOT Act that was reported unanimously out of Committee. The final version of the USA PATRIOT Act, however, adopted the Senate language that did not include this provision.

This section would also ensure that providers of communications remain covered under 18 U.S.C. § 2511(2)(a)(ii), another "no cause of action" provision which protects providers from law suits when they are legally assisting law enforcement with an investigation under the new computer trespasser provision, § 2511(2)(i), created in the USA PATRIOT Act.

Sec. 108. Emergencies.

This section amends 18 U.S.C. § 3125(a)(1) to expand when law enforcement may use pen registers and trap and trace devices in an emergency situation. Law enforcement uses pen registers and trap and trace devices to provide information about the source or destination of a communication without capturing the content of the communication. This is the least invasive method of surveillance of electronic communications and is indispensable to investigations. Trap and trace devices can identify, for example, the source of phone calls placed by a kidnapper in order to identify his whereabouts. In ordinary circumstances, any attorney for the Government may obtain a pen/trap order by certifying to a court that the information collected will be relevant to a criminal investigation. In an emergency, law enforcement authorities may install a pen/trap device for forty-eight hours while court authorization is sought.

This amendment expands the list of situations during which an emergency pen/trap can be used by adding immediate threats to national security interests and ongoing attacks on protected computers. Under current law, threats to national security interests already justify the emergency use of a full-content wiretap—a much more invasive tool than a pen/trap.[6]

The Committee notes that this section in no way changes the limitations under current law on the emergency use of this authority. Those limitations are: (1) a Government official authorizing an emergency pen/trap must determine that there are grounds upon

[6] 18 U.S.C. § 2518 (7)(a)(ii).

which a court could enter a pen/trap order;[7] (2) emergency authorization lasts only forty-eight hours, within which time a court order must be obtained for the surveillance to continue;[8] and (3) it is a violation of the statute to fail to apply for an order within forty-eight hours of installation or use of the device.[9]

Sec. 109. Protecting Privacy.

Section 109(a) would amend 18 U.S.C. § 2511(4)(b) to raise the penalties for a person who illegally intercepts cell-phone conversations. Under current law, § 2511(4)(b) provides lesser penalties for certain wiretap violations. For example, while most illegal wiretapping constitutes a 5-year felony, the statute punishes first time offenders who intercept a cellular phone call with a mere fine. The requirement that violations be committed intentionally[10] ensures that mere inadvertent overhearing of a brief portion of a communication is not criminalized. The Committee believes that the special penalty scheme for cell phone violations should be eliminated and that all wire interceptions should be treated equally. Therefore, this section makes the statutory maximum penalty for all such offenses the same regardless of the technology used.

Section 109(b) amends 18 U.S.C. § 2701 to increase penalties for a person who invades the privacy of another person's stored communications. Under current law, subsection 2701(b) defines the penalties when an individual invades the privacy of others by accessing communications in "electronic storage." Such privacy invasions include, for example, the reading of an e-mail stored on an e-mail server awaiting delivery to its recipient. Thus, a system administrator for a company would violate this provision if, outside of his regular duties, he used his access to the computer system to read the CEO's e-mail and use the information contained in those e-mails for his own financial gain.

The Committee believes that this section is necessary because current law punishes what are often very significant privacy invasions as misdemeanors. Under current law, where the invasion of privacy occurs for commercial gain or advantage or malicious destruction, the maximum penalty is 1 year imprisonment for first time offenders. Violators without these mental states receive a maximum of 6 months in jail. The current penalty structure, in which all first-time offenses are misdemeanors, does not adequately reflect the seriousness of the offense. According to the Department of Justice, few (if any) prosecutions have been brought for this violation, limiting the deterrent effect of the statute. In addition, in order to qualify for the enhanced penalty provision, a violator must have the intent to cause damage or to benefit financially from the action. This list of aggravating mental states does not include those who violate the statute in furtherance of any criminal or tortious act.

The amendments to 2701(b) raise the maximum criminal penalties to 5 years where the actor has the aggravating mental state (ten years for repeat offenders) and to 1 year for other violations (five years for repeat offenders). The amendments would assure

[7] 18 U.S.C. § 3125(a)(2).
[8] 18 U.S.C. § 3125(b).
[9] 18 U.S.C. § 3125(c).
[10] See 18 U.S.C. § 2511(1)(a)-(d).

that individuals who violate this section in furtherance of some other criminal or tortious act are appropriately punished. The Committee believes this change in the law will provide judges with the flexibility and discretion to impose more serious penalties for more serious crimes.

Section 109(c) amends 18 U.S.C. § 3105, a 1917 provision, to clarify that a law enforcement officer does not need to be present for a warrant to be serviced or executed under the Electronic Communications Privacy Act (ECPA). Due to the nature of electronic communications, much of this information is in the possession of Internet Provider Services (ISPs) and law enforcement officials often serve such warrants over facsimile machines and are not present at the site of the ISP. In a recent child pornography case, a Minnesota Federal district court, in *U.S.* v. *Bach*,[11] however, ruled that this procedure was an unreasonable search and seizure. The Court found that a police officer had to be present at the time. This subsection makes it clear that a police officer does not have to be present at the time a warrant is served under ECPA.

TITLE II—OFFICE OF SCIENCE AND TECHNOLOGY

Sec. 201. Establishment of Office; Director.

This section establishes the Office of Science and Technology (OST) as an independent office. The office will be under the general authority of the Assistant Attorney General, Office of Justice Programs (OJP), and shall no longer be housed in the National Institute of Justice (NIJ).

The mission of the OST is to provide State and local law enforcement access to new technologies and to help develop those new technologies. Currently, OST is housed in NIJ, which was created in 1968, in the Omnibus Crime Control and Safe Streets Act to support Federal criminal justice research. The mission of NIJ is to improve police work and the judicial system and to gain a better understanding of criminal behavior. NIJ was created when technology was not the overriding priority. Today, technology is a priority and the establishment of OST as an independent office will ensure that technology is treated as a priority.

The Committee believes that there is a need for a real reform of the OJP programs and the way those programs are managed. The change proposed by this bill is part of a larger restructuring process. It will help the OJP to focus the necessary resources on the development of technology and hard science research.

At hearings held on reforming OJP, the former Assistant Attorney General for OJP, Laurie Robinson, testified that this is one area OJP really needs to reorganize. States need to have a more clear direction as to how and where to obtain technology grants. This section will assist that process. Additionally, the Committee believes that this change will help focus at OJP on the important area of technology research and at the same time maintain the core functions for which NIJ was established.

Today, the duties of NIJ are to:

- [research] the nature and impact of crime and delinquency;

[11] *United States* v. *Bach*, No. 01–221, (PAM/ESS) 2001 U.S. Dist. LEXIS 21853 (D. Minn. Dec. 14, 2001).

- [develop] applied technologies, standards and tools for criminal justice practitioners;
- [evaluate] existing programs and responses to crime;
- [test] innovative concepts and program models in the field;
- [assist] policymakers, program partners, and justice agencies; and
- [disseminate] knowledge to many audiences.[12]

NIJ would continue to carry out all of its functions except for the development of applied technologies, standards, and tools. These would be the responsibilities of OST. Additionally, one of the NIJ's responsibilities is to evaluate existing programs. To avoid a conflict of interest and allow NIJ to evaluate the work of OST, it makes sense to transfer OST outside of NIJ. This change will allow NIJ to maintain its integrity as an independent evaluator of OJP.

Sec. 202. Mission of Office; Duties.

This section establishes the mission and duties of OST to serve as the national focal point to improve law enforcement technology and to make technical assistance available to Federal, State, and local law enforcement agencies. This section was modified by the Committee with regard to subsections (3) and (4) to clarify that OST may use input from industry in developing technology standards; however, the Committee does not intend this modification to prevent OST from independently developing whatever standards it deems appropriate for law enforcement technology and equipment.

This section requires the Office to award research and development work on a competitive basis. Additionally, it requires the Director of the OST to provide to Congress a needs assessment for Federal, State and local law enforcement and a strategic plan for meeting those needs.

Sec. 203. Definition of Law Enforcement Technology.

This section defines "law enforcement technology" to include 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.

This section transfers OST and all of its assets and personnel out of the NIJ within OJP to be a separate office within OJP. The Attorney General shall have the authority under this section to transfer any other program or activity he or she determines is appropriate for this office and provide a report to Congress on its implementation after 1 year. The Committee believes that the Attorney General should review all law enforcement technology programs within the Department, including such programs as the Office of Community Oriented Policing Services (COPS).

Sec. 205. National Law Enforcement And Corrections Technology Centers.

This section requires the Director of the OST to operate and support National Law Enforcement and Corrections Technology Cen-

[12] http://www.ojp.usdoj.gov/nij/about.htm (June 6, 2002).

ters. These centers support research, development, and implementation of technology to assist law enforcement. This bill will require the Director of the OST to make recommendations regarding the effectiveness of the centers and the need for additional centers.

Presently, OST uses the existing National Law Enforcement and Corrections Technology Centers as one of the primary mechanisms to accomplish its mission. Currently, there are five regional centers and one national office.

Sec. 206. Coordination with Other Entities within Department of Justice.

This section provides that the Assistant Attorney General shall coordinate the activities of the various bureaus whose functions relate to technology programs. In several hearings regarding the operations of OJP, it became apparent that the lack of coordination among the various bureaus and offices at OJP creates confusion and unnecessary duplication. The Committee believes that requiring more coordination among the various offices will increase efficiency and effectiveness of the programs.

AGENCY VIEWS

U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

February 12, 2002

The Honorable Lamar S. Smith
Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter presents the views of the Justice Department on H.R. 3482, the "Cyber Security Enhancement Act of 2001." We appreciate efforts, like those embodied in title I of the bill, to bolster the enforcement regime for computer crime. In particular, we support title I's directive to the United States Sentencing Commission to amend computer crime sentencing guidelines. However, we strongly oppose title II because of provisions separating the Office of Science and Technology from the National Institute of Justice. Below, we offer several suggestions for improving the drafting of title I.

Title I: Computer Crime

Section 101. Section 101 of the bill would require the United States Sentencing Commission to "amend the federal sentencing guidelines" but at the same time states that the commission "if appropriate, [will] promulgate guidelines or policy statements." This directive appears to be both mandatory and discretionary. In addition, the directive is unclear about what the commission is expected to review and what the concerns of the Congress are. We recommend the directive be revised as follows, adding several factors for the commission's consideration:

> "Section 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 paragraph (a), the growing incidence of such offenses, and the need for aggressive and appropriate law enforcement action and an effective deterrent to prevent such offenses;

"(2) consider the increase in the maximum penalties for offenses under section 1030(a)(5), as amended by the USA PATRIOT Act, P.L. 107-56;

"(3) consider the following factors and how they should be considered in sentencing a person convicted of such an offense:

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

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

"(C) whether or not the offense was committed for purposes of commercial advantage or private financial benefit;

"(D) whether or not 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 by the offense;

"(F) whether the offense involved a computer used by the Federal 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 of safety, or injury to any person; and

"(4) consult with appropriate law enforcement and computer crime experts;

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

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

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

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

"Section 101A. Study And Report on Computer Crimes.

"DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.- Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress on matters addressed by this legislation. The report shall explain the changes, if any, to sentencing policy made by the Sentencing Commission in response to this Act and include any recommendations that the Commission may have for retention or modification of current penalty levels, including statutory penalty levels, for computer crimes."

Section 102. We believe the changes section 102 would make to 18 U.S.C. § 2702(b) require an additional technical change: striking "or" at the end of subparagraph (6)(B) of section 2702(b) and inserting "or" after subparagraph (6)(A).

We propose the following language:

"(5) in paragraph (6), by striking "or" following subparagraph (B) and inserting "or" following subparagraph (A);

Section 104. Section 104(a) of the bill would direct the Attorney General, "acting through the Federal Bureau of Investigation," to establish and maintain the National Infrastructure Protection Center to serve as a national focal point for threat assessment and warning and investigation of and response to attacks on the Nation's critical infrastructure from physical and cyber sources. The Administration requests that the phrase ", acting through the Federal Bureau of Investigation," be stricken from section 104(a). Statutes that grant authority to the Attorney General should not limit which of his subordinate officers or organizations in the Department of Justice through which he can act.

Section 105. Section 105 attempts to address a serious loophole in the statute prohibiting the distribution of advertisements for illegal interception devices. However, the language used refers to a "publication" of some sort and we are concerned that a loophole might continue to

exist. Today, one can advertise illegal interception devices through such means as e-mail spam that may not clearly constitute a "publication". Similarly, one could distribute advertisements on computer networks that are not part of the Internet (such as AOL's proprietary network). To ensure that these other means of distribution are covered, we propose the following language for 18 U.S.C. § 2512(1)(c):

> (c) places in any newspaper, magazine, handbill, or other publication ***or disseminates by electronic means*** any advertisement of--
>
> (i) any electronic, mechanical, or other device knowing or having reason to know...

Section 106. Section 106 would establish higher statutory maximum penalties for "knowingly" causing death or serious bodily injury. This important amendment would address a serious type of offense not covered in other areas of the criminal code. We have several suggestions regarding the drafting of this provision.

We are concerned that using the term "knowingly" would preclude increased penalties where the offender's actions *recklessly* caused death or serious injury. Where the person intentionally creates an unreasonable or unjustifiable risk that death will result, we believe that person should be eligible for the increased punishment. Therefore, we suggest the following language for 1030(c)(5):

> (5) (A) if the defendant knowingly or recklessly causes or attempts to cause serious bodily injury from acts committed in violation of subsection (a)(5)(A)(i), a fine under this title, imprisonment for not more than twenty years, or both; and
>
> (B) if the defendant knowingly or recklessly causes or attempts to cause death from acts committed in violation of subsection (a)(5)(A)(i), a fine under this title, imprisonment for any term of years or for life, or both.[1]

We also suggest defining "serious bodily injury" in 18 U.S.C. 1030(e)(13) as follows:

> (13) the term "serious bodily injury" has the meaning set forth in section 2119(2).

---

[1]We note that our proposed change would include changing language currently in section 106 from "injury from *acts committed in violation* of subsection (a)(5)(A)(i) . . ." (emphasis added) to "injury *in a violation* of subsection (a)(5)(A)(i) . . ."

Section 107. We believe section 107 requires two technical modifications. First, we think a comma should be added before "statutory authorization" in subsection (a), so that it would state ", statutory authorization". Second, we think subsection (b) should state the following:

> "(b) SECTION 2511.–***The penultimate line of*** section 2511(2)(a)(ii) of title 18, United States Code, is amended by inserting ", statutory authorization" after "court order".

Title II: Office of Science and Technology

Title II would establish the Office of Science and Technology ("OST") as a new directorate within the Office of Justice Programs. This new directorate would be independent of the National Institute of Justice ("NIJ"). The director would be a member of the career Senior Executive Service. We oppose title II in its entirety and strongly recommend that it be deleted.

The Office of Science and Technology is an integral, component part of the NIJ, the Nation's resource for crime and justice research and development, be it social science research and evaluation or technology research and development. We strongly believe that the OST should remain part of NIJ.

Improving service to customers of the Office of Justice Programs ("OJP") is a driving force behind this Administration's effort to reorganize OJP – an effort years in the making. Title II is directly at odds with this objective. Currently, all aspects of NIJ's research, whether social science or technology research, are focused upon benefitting the same set of customers: State and local policymakers and practitioners. In some cases, customers seek information that crosses the boundaries between social science and technology research. As a unified agency, NIJ avoids artificially limiting dialogue with customers to one type of science or another. Additionally, maintaining NIJ as a unified agency decreases the likelihood that customers need to seek information from multiple offices within the Justice Department.

By having all research disciplines available to the NIJ director, the director is able to prepare a comprehensive program to tackle important policy or practitioner problems. The director also is able to marry newly-developed technologies with the social, legal, and organizational ramifications of the use of those technologies in the "real world." For example, a comprehensive counterterrorism research program necessarily contains technology research and research studies drawing on the social and behavioral sciences. Similarly, the successful use of surveillance technologies and crime mapping applications at the local level is highly dependent on non-technology factors that should be addressed during the research phase and not after all the funds have been spent.

Also, a separate OST inevitably would increase administrative support costs as some NIJ functions would cease to be shared. For example, the NIJ director is served by a deputy director, an executive assistant, a science advisor, and other staff members that meet the administrative, budgetary, and strategy planning needs of all of the NIJ. Additionally, the NIJ has a newly-

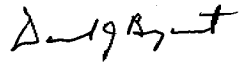
developed grants monitoring software program that all of its staff members use, as well as shared physical facilities (such as conference rooms) that its staff uses. If OST were separated from NIJ, these resources would have to be duplicated at considerable cost.

Both the stature of a politically-responsible appointment and the legislative authorities and responsibilities assigned to the NIJ director attracts highly-qualified and experienced persons to lead NIJ and also makes NIJ accountable for generating the knowledge and tools needed by law enforcement. This stature and accountability would be diminished if the OST were headed by a lower-ranking, career official.

Conclusion. We oppose title II in its entirety and strongly recommend that it be deleted. Even within the current organizational structure, we do not support any expansion of OST's role regarding the development and application of forensic technology. We would be happy to meet with you or your staff to better understand congressional concerns in this area and look for constructive solutions.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that, from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,



Daniel J. Bryant
Assistant Attorney General

cc: The Honorable Bobby Scott
Ranking Minority Member

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

§ 1030. Fraud and related activity in connection with computers

(a) * * *

* * * * * * *

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1) * * *

* * * * * * *

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; **[**and**]**

(4)(A) *except as provided in paragraph (5),* a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) *except as provided in paragraph (5),* a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section**[**.**]***; and*

(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.

* * * * * * *

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

* * * * * * *

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) * * *

(2)(a)(i) * * *

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) * * *

* * * * * * *

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, *statutory authorization,* or certification under this chapter.

* * * * * * *

(4)(a) * * *

[(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for pur-

poses of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then—

[(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

[(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.]

[(c)] *(b)* Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) * * *

* * * * * * *

§ 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally—

(a) * * *

* * * * * * *

(c) places in any newspaper, magazine, handbill, or other publication *or disseminates by electronic means* any advertisement of—

(i) any electronic, mechanical, or other device *knowing the content of the advertisement and* knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

* * * * * * *

§ 2520. Recovery of civil damages authorized

(a) * * *

* * * * * * *

(d) DEFENSE.—A good faith reliance on—

(1) * * *

* * * * * * *

(3) a good faith determination that section 2511(3) *or 2511(2)(i)* of this title permitted the conduct complained of;

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * * * *

§ 2701. Unlawful access to stored communications

(a) * * *

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain*, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State*—

(A) a fine under this title or imprisonment for not more than [one year] *5 years*, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than [two years] *10 years*, or both, for any subsequent offense under this subparagraph; and

[(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.]

(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.

* * * * * * *

§ 2702. Voluntary disclosure of customer communications or records

(a) * * *

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.— A provider described in subsection (a) may divulge the contents of a communication—

(1) * * *

* * * * * * *

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; [or]

(6) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; *or*

(B) if required by section 227 of the Crime Control Act of 1990; or

[(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.]

(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.

* * * * * * *

§ 2703. Required disclosure of customer communications or records

(a) * * *

* * * * * * *

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena*, statutory authorization*, or certification under this chapter.

* * * * * * *

PART II—CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 205—SEARCHES AND SEIZURES

* * * * * * *

§ 3105. Persons authorized to serve search warrant

A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution. *The presence of an officer is not required for service or execution of a warrant under section 2703 when the provider of electronic communications service or remote computing service produces the information required in the warrant.*

* * * * * * *

CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

* * * * * * *

§ 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the

Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(1) an emergency situation exists that involves—

(A) immediate danger of death or serious bodily injury to any person; **[**or**]**

(B) conspiratorial activities characteristic of organized crime**[**,**]***;*

(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;

* * * * * * *

SECTION 102 OF THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

DUTIES AND FUNCTIONS OF ASSISTANT ATTORNEY GENERAL

SEC. 102. (a) The Assistant Attorney General shall—

(1) * * *

* * * * * * *

(5) *coordinate and* provide staff support to coordinate the activities of the Office and the Bureau of Justice Assistance, the National Institute of Justice, the Bureau of Justice Statistics, and the Office of Juvenile Justice and Delinquency Prevention; and

* * * * * * *

MARKUP TRANSCRIPT

BUSINESS MEETING

WEDNESDAY, MAY 8, 2002

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in Room 2141, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr. [Chairman of the Committee] presiding.

Chairman SENSENBRENNER. [Presiding.] The Committee will be in order.

When the Committee last recessed, the Judicial Improvement Act had been favorably reported.

The next item on the agenda is H.R. 3482, the "Cyber Security Enhancement Act of 2001." The Chair recognizes the gentleman from Texas, Mr. Smith, Chairman of the Subcommittee on Crime, Terrorism, and Homeland Security, for a motion.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, the Subcommittee on Crime, Terrorism, and Homeland Security reports favorably the bill H.R. 3482 with a single amendment in the nature of a substitute and moves its favorable recommendation to the full House.

Chairman SENSENBRENNER. Without objection, the bill will be considered as read and open for amendment at any point. And the Subcommittee amendment in the nature of a substitute, which the Members have before them, will be considered as read and considered as the original text for purposes of amendment.

[The amendment follows:]

SUBCOMMITTEE AMENDMENT IN THE NATURE OF SUBSTITUTE TO H.R. 3482

Strike all after the enacting clause and insert the following:

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.

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); and

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

(4) by striking the period at the end of paragraph (6) and inserting ''; or''; and

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

''(7) to a 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 of the information without delay.''.

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. NATIONAL INFRASTRUCTURE PROTECTION CENTER.

(a) IN GENERAL.—The Attorney General shall establish and maintain a National Infrastructure Protection Center (hereinafter in this section referred to as the ''Center'') to serve as a national focal point for threat assess-

ment, warning, investigation, and response to attacks on the Nation's critical infrastructure for both physical and cyber sources.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for fiscal year 2003 to carry out this section, $125,000,000.

SEC. 105. 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'';

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

(3) by inserting ''or transmitted'' after ''transported''; and

(4) by inserting ''or communication'' after ''foreign commerce''.

SEC. 106. 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. 107. PROVIDER ASSISTANCE.

(a) SECTION 2703.—

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

(2) Section 2703(f) of title 18, United States Code, is amended by adding at the end the following:

"(3) REMEDIES.—If a provider of wire or electronic communication services or a remote computing service intentionally fails to comply with a request under this subsection, the requesting governmental entity may obtain appropriate relief in a civil action, in addition to any other remedy or cause of action that entity may have.".

(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.

(c) SECTION 2706.—

(1) Section 2706(a) of title 18, United States Code, is amended by inserting "requesting or" after "entity" the first place it appears.

(2) Section 2706(b) of title 18, United States Code, is amended by inserting "assembling or" after "person or entity".

SEC. 108. 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 that constitutes a crime punishable by a term of imprisonment greater than one year;".

SEC. 109. PROTECTING PRIVACY.

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

(1) in paragraph (a), by striking "paragraph (b) of this subsection or";

(2) by striking paragraph (b); and

(3) 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.''.

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 ap-

proval 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 used by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), which may, in the discretion of the Office, allow for supplier 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 sub-

1 section (a)(5) by inserting ''coordinate and'' before ''pro-
2 vide''.

Chairman SENSENBRENNER. The Chair recognizes the gentleman from Texas, Mr. Smith, to strike the last word.

Mr. SMITH. Thank you, Mr. Chairman.

H.R. 3482, the "Cyber Security Enhancement Act of 2002," will strengthen penalties to better reflect the seriousness of cyberattacks. It will assist State and local law enforcement through better grant management, accountability, and dissemination of technical advice and information; will help protect the Nation's critical infrastructure; and will enhance privacy protections. H.R. 3482 was approved by the Subcommittee on a voice vote.

Last summer, the Subcommittee on Crime held three hearings on the growing threat of cybercrime and cyberterrorism. In fact, the Subcommittee held more hearings on the subject of cybercrime than any other issue. Cybercrime knows no borders or restraints and can harm the Nation's economy and endanger the public's health and safety.

Cybercrime is a growing concern, but many are reluctant to report it. A recent survey conducted by the FBI and the Computer Security Institute revealed most corporations and Government agencies had been victims of computer hackers, but they rarely report these security breaches to authorities.

While nearly 90 percent of the respondents detected breaches in the last year, only 34 percent reported the attacks. Common forms of attack included denials of services, viruses and worms, financial fraud, and Web site defacement.

But businesses and Government agencies aren't the only victims. Last year, Mr. Chairman, nearly 10,000 Americans reported losing $18 million on online scams. Law enforcement officials and private industry representatives agree that better coordination, cooperation, and information sharing are needed, as well as stronger penalties for cyberattacks.

In this legislation, penalties are strengthened by directing the United States Sentencing Commission to review and, if appropriate, amend its guidelines to provide a wider range of criteria in sentencing cybercrimes. It also increases penalties for those who cause or attempt to cause death or serious bodily injury through cyberattacks.

This bill contains provisions that protect Internet service providers who, for example, share information about potential terrorist attacks when they legally assist law enforcement officers under the new USA PATRIOT Act.

Finally, the bill helps protect the Nation's critical infrastructure by providing State and local law enforcement personnel access to new technologies through better grant management and accountability.

So, Mr. Chairman, I urge my colleagues to support this bill and yield back the balance of my time.

Chairman SENSENBRENNER. Without objection, all Members may insert opening statements in the record at this point in time.

And since there are no Members from the minority present, without objection, we will set this bill temporarily aside, because I know that there are some amendments that the minority wishes to offer.

Well, I see the gentleman from Virginia present.

Are there amendments?

Ms. HART. Mr. Chairman?

Mr. SMITH. Mr. Chairman, I have——

Ms. HART. Mr. Chairman?

Chairman SENSENBRENNER. Does the gentleman from Texas, the Subcommittee Chair, have an amendment?

Mr. SMITH. Yes, Mr. Chairman. I ask unanimous consent that my amendment in the nature of a substitute be considered as read.

Chairman SENSENBRENNER. Already been given—the gentleman from Texas has an amendment at the desk.

The Clerk will report the amendment.

The CLERK. Amendment in the nature of a substitute to H.R. 3482. Strike all after the enacting clause and insert the following——

Chairman SENSENBRENNER. Without objection, the amendment will be considered as read and open for amendment at any point.

[The amendment follows:]

AMENDMENT IN THE NATURE OF SUBSTITUTE TO H.R. 3482

Strike all after the enacting clause and insert the following:

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.

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); and

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

(4) by striking the period at the end of paragraph (6) and inserting ''; or''; and

(5) 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.''.

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. NATIONAL INFRASTRUCTURE PROTECTION CENTER.

(a) IN GENERAL.—The Attorney General shall establish and maintain a National Infrastructure Protection Center (hereinafter in this section referred to as the ''Cen-

ter'') to serve as a national focal point for threat assessment, warning, investigation, and response to attacks on the Nation's critical infrastructure for both physical and cyber sources.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for fiscal year 2003 to carry out this section, $125,000,000.

SEC. 105. 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. 106. 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. 107. 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. 108. 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. 109. 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.''.

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 ap-

proval 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 used by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), which may, in the discretion of the Office, allow for supplier 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 sub-

1 section (a)(5) by inserting ''coordinate and'' before ''pro-
2 vide''.

Chairman SENSENBRENNER. And without objection, this amendment in the nature of a substitute will be considered the original text for purposes of amendment.

Hearing no objection, so ordered.

The gentleman from Texas is recognized for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman.

I offer this amendment in the nature of a substitute at the suggestion of legislative counsel. This amendment makes only a few discrete changes to the bill.

First, section 102 is amended at the request of the Center for Democracy and Technology. The amendment clarifies that if a communication provider believes in good faith that a life-threatening emergency exists and discloses electronically stored information relating to the emergency to a Federal, State or local government official, then the provider will not be held liable.

Second, section 105 is amended technically to clarify that dissemination by electronic means is another form of publication.

Third, section 107 is amended to strike the reimbursement provisions in the remedies section. Neither industry nor the Department of Justice have been able to agree on the nature of the problem here or on a solution. It will be better to request a study by the General Accounting Office on both the issue of compliance by communication providers and preserving records and the issue of reimbursement by the Government entities that request the providers' compliance.

Mr. Chairman, I believe this amendment strengthens the bill and urge my colleagues to support it.

I yield back the balance of my time.

Chairman SENSENBRENNER. Are there any amendments to this new amendment in the nature of a substitute?

The gentleman from Virginia.

Mr. SCOTT. Mr. Chairman, I have an amendment at the desk.

Chairman SENSENBRENNER. The clerk will report the amendment. Is the clerk clear which amendment to report?

Mr. SCOTT. I just have one.

Chairman SENSENBRENNER. The clerk will report the amendment.

The CLERK. Amendment to the amendment in the nature of the substitute to H.R. 3482, offered by Mr. Scott. On page 4, at the end of section 102, insert the following new subsection: (c) Reporting of disclosures——

Chairman SENSENBRENNER. Without objection, the amendment is considered as read.

[The amendment follows:]

Scott Amendment to the Amendment in the Nature of a Substitute to H.R. 3482

#2

On Page 4, at the end of section 102, insert the following new subsection:

(c) **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.**

Chairman SENSENBRENNER. And the gentleman from Virginia is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

I'm pleased to join you in convening this markup of the cybersecurity act of 2001. And generally, I support the concept of allowing Internet service providers to give information to law enforcement officials when there is an emergency—of death or serious bodily injury.

Under the current law, an ISP can only release information if it reasonably believes that immediate danger exists. And I support that change, too—believe it's in good faith.

If the FBI presents information that the ISP believes, if true, could present a threat of death or serious injury, the ISP dispatcher on duty shouldn't have to wake up the corporate counsel to determine what to do. They ought to give up the information. If there's time to do all the—check with the corporate counsel, then the FBI could have just gone to the magistrate or judge and gotten a search warrant.

Mr. Chairman, I agree with the bill. This amendment clarifies one part of it. It's been, as I understand it, worked with staff, requiring reporting disclosures, so that the Attorney General will report each year how often these procedures are used, so we have some handle on what we're dealing with.

Ms. LOFGREN. Would the gentleman yield for a question?

Mr. SCOTT. I yield.

Ms. LOFGREN. Is it the intent of the amendment that this publication would be the number but not necessarily the entities that disclose? There'd be anonymity, a compilation, or not?

Mr. SCOTT. It says the number of customers or subscribers, not the name of the customer or subscriber.

Ms. LOFGREN. Well, it says: report to the Attorney General, stating the subparagraph under which the disclosure was made.

I think it's ambiguous. I want to make sure—I think it's fine to have a compilation, but if we have the individual entities, I think it would be a deterrent.

Mr. SCOTT. The intent is the number of customers or subscribers whom the information disclosed pertained, the number of communications. Where it says "entity," that's the Government entity.

Ms. LOFGREN. Okay, thank you very much.

Mr. SCOTT. Thank you.

Chairman SENSENBRENNER. Does the gentleman yield back?

Mr. SCOTT. I yield back.

Chairman SENSENBRENNER. The gentleman from Texas?

Mr. SMITH. Mr. Chairman, I'm going to express a couple of concerns about this amendment.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman.

Let me ask the gentleman from Virginia—and I will say that I haven't seen this amendment until right now, and it comes as a surprise to me—that it seems to me—a couple of the concerns that I had would be, first of all, unfunded mandates, in the sense that we're adding burdens to State and local governments to compile all this information. And I sort of have a Constitutional objection to that.

It also seems that we're setting a precedent here in requiring reports that might impose a burden on the Administration and just add to the bureaucracy rather than solving any particular problem.

And I appreciate what the gentleman is trying to do. But as I recall, if the gentleman is trying to find out whether there's been an abuse of the process or whether there's been violations of an individual's civil liberties and so forth, that just reporting the items that the gentleman has in this amendment is not going to necessarily disclose that. And so what I would like to do is to work in good faith with the gentleman to refine the language, so that we can—if the gentleman—and it's a worthy goal—try to ferret out any abuse by law enforcement officials without overreaching.

Mr. SCOTT. Will the gentleman yield?

Mr. SMITH. I'd be happy to yield.

Mr. SCOTT. This anticipates that if a Government entity takes advantage of the section, within 90 days, they'll report that fact to the Attorney General. And the Attorney General shall publish a 1-year summary, a single report, not an annual report, a single report, so that we can get a handle on what happened during the first year of the use of this section.

It is not anticipated that this section would be used very often, so there shouldn't be—if there is in fact an administrative burden, that means it is being used a lot more than you and I anticipate that it would be used.

But we just say that, if the Government entity gets information, they'll just let the Attorney General know, and the Attorney General will wrap it up in one report and publish it, so it should not be a burden.

Mr. SMITH. Well, it may not be as much of a burden as it would be if they were doing these reports on a regular basis.

Mr. Chairman, I think I am not going to object to this amendment and urge my colleagues to support it, with the understanding, I might say, if I may engage the gentleman from Virginia in a colloquy, that he is not going to seek to do this in future years; this will be a one-time evaluation of the process.

Mr. SMITH. Well, the expectation is that, if things go well, you would not need to. But if there is abuse—you would have to pass a new law to get an additional—additional reports. So, I mean, the thing essentially sunsets itself.

Mr. SMITH. Okay.

Okay, Mr. Chairman, I'm going to acknowledge that my colleague from Virginia is acting in good faith and not trying to increase the burden on the Government, and I won't object to this.

Chairman SENSENBRENNER. The question is on the Scott amendment to the amendment in the nature of a substitute.

Those in favor will say aye.

Opposed, no.

The ayes appear to have it. Thy ayes have it, and the amendment to the amendment in the nature of a substitute is agreed to.

Are there further amendments?

Ms. HART. Mr. Chairman?

Chairman SENSENBRENNER. The gentlewoman from Pennsylvania.

Ms. HART. Mr. Chairman, I have an amendment at the desk.

Chairman SENSENBRENNER. The Clerk will report the amendment.

The CLERK. Amendment to the Subcommittee amendment in the nature of a substitute to H.R. 3482, offered by Ms. Hart, Mr. Berman, and Ms. Lofgren.

Chairman SENSENBRENNER. Without objection, the amendment is considered as read.

[The amendment follows:]

AMENDMENT TO SUBCOMMITTEE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 3482 OFFERED BY MS. HART, MR. BERMAN, AND MS. LOFGREN

Page 7, after line 18, insert the following:

(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 warrant under section 2703 when the provider of electronic communications service or remote computing service produces the information required in the warrant.".

Chairman SENSENBRENNER. And the gentlewoman from Pennsylvania is recognized for 5 minutes.

Ms. HART. Thank you, Mr. Chairman.

My amendment is also sponsored by Mr. Berman and Ms. Lofgren. It addresses an ambiguity in the current law for warrants issued under the Electronic Communications Privacy Act. The amendment also addresses issues we raised in the passage of the USA PATRIOT Act. It would clarify that a law enforcement officer does not need to be present for a warrant executed under the Electronic Communications Privacy Act.

With increased communications through e-mail and other activities on the Internet, acquiring access to this information is essential for any successful investigation. Much of this information is in the hands of a third party ISP, and law enforcement must obtain

this information directly from that ISP. While the ECPA search warrants are issued by neutral magistrates, they are not generally executed like traditional search warrants. Law enforcement officials do not routinely enter the ISP's centers; rather, the ISP accepts the warrant, assigns it to network technicians to search for the requested information, then delivers that information in a suitable format to the officer.

Recently, though, a Michigan Federal district court, in *U.S.* v. *Bach*, ruled that an officer must actually be present during the execution of the ECPA search warrants. That really does change what practice has been.

The court had applied a provision originally passed in 1917, which is intended to require officers to be present during the execution of coercive, physical search. Not only has this notion never before been recognized by a court, but it raises a variety of additional problems that my amendment would seek to resolve.

First, the 1917 provision was designed to protect privacy, but application of that provision to the ECPA warrant actually hinders individual privacy. If an officer is required to be present during the execution of that warrant, they will have access to all information, including the information of additional consumers who aren't named in that warrant, that is, that the ISP's technician has to review to fill the requirements of the warrant. The court's ruling actually harms the privacy rights of individuals.

Second, requiring that an officer be present raises a variety of practical problems for the execution of the warrant. Investigations will be halted until a law enforcement officer arrives at each location. More than one ISP may have relevant information, and that information may be stored in more than one location, meaning that an officer must be at each location. This is a drain on the resources of law enforcement agencies.

Third, the requirement imperils any pending case where a law enforcement official has acquired information from an ISP without meeting the requirement established by that court.

Finally, this amendment is practical, as it puts into law established and very workable practice. A large ISP may receive as many as 500 requests a month for what is fairly straightforward information.

To require law enforcement to be present when each amendment is executed is not practical.

The amendment clarifies, again, that an officer need not be present during the execution of a warrant granted under the ECPA. It helps law enforcement, it helps ISPs, and most importantly, it protects the private information of the consumers that are involved with that ISP.

And I ask for the support of the amendment, and I yield back.

Chairman SENSENBRENNER. The gentlewoman from California.

Ms. LOFGREN. Mr. Chairman, I am strongly supportive of this amendment.

Chairman SENSENBRENNER. The gentlewoman is recognized for 5 minutes.

Ms. LOFGREN. I want to thank my colleagues, Mr. Berman and Ms. Hart, for co-sponsoring it.

And I think this is a perfect example of how laws created long ago for the off-line world really don't make any sense in the online world. It doesn't make a lot of sense that law enforcement that should be present in a physical search, because they have, potentially, a role to play, would have to be present, overlooking a technician's should and, for the most part, not even understanding, probably, what that technician is doing.

So I think this does no harm and certainly does a lot of good in being efficient. And I strongly support the amendment and thank the gentlelady for taking the lead on this, and would yield additional time to Mr. Berman.

Mr. BERMAN. I thank the gentlelady for yielding, and I'll be very brief, because I think the author of the amendment described it quite completely and well.

It's a direct result of a court interpretation, and it's somewhat counterintuitive, because while you might normally want to think that it makes sense to have an officer serve the warrant, when you're dealing with the ISPs, they're getting thousands of warrants, so it's very inefficient in terms of time. But it also raises some privacy concerns, because it allows that officer to have access to communications that are outside the scope of the investigation.

So both from an efficiency point of view and a privacy point of view, I think this amendment is appropriate and urge its passage. And I yield back to the gentlelady.

Ms. LOFGREN. Thank you. And, Mr. Chairman, to avoid asking for an additional 5 minutes, I would also like to praise the underlying bill, the provision establishing the National Law Enforcement Corrections Technology Center.

Recently, I had occasion to try and discover, or at least have validated, a technology that is being deployed for biometrics. And there's a lot of technology in Silicon Valley; this is a technology that is not coming out of Silicon Valley. In fact, it's licensed to a firm in Massachusetts—having to do with iris scans. And it looks to be the cheapest and most reliable form of biometrics.

And yet, we would not want to deploy it without some kind of assessment or validation from a disinterested party. I asked NIST to take a look at the technology and to tell me whether or not it was as good as it appeared and was claimed.

But I would just like to note that the establishment of this National Law Enforcement Corrections Technology Center in the underlying bill is an excellent advance to make sure that we are deploying the right technology in law enforcement as well as other security agencies.

So not only will this amendment make the execution of warrants tech-friendly, the underlying bill also improves it.

And I yield back my time.

Chairman SENSENBRENNER. The question is on agreeing to the amendment offered by the gentlewoman from Pennsylvania.

Those in favor will say aye.

Opposed, no.

The ayes appear to have it. The ayes have it, and the amendment is agreed to.

Are there further amendments?

If there are no further amendments, the Chair notes the presence of a reporting quorum. The question is on the amendment in the nature of a substitute as amended.

Those in favor will say aye.

Opposed, no.

The ayes appear to have it. The ayes have it.

The question now occurs on the motion to report the bill H.R. 3482 favorably as amended by the amendment in the nature of a substitute.

All in favor will say aye.

Opposed, no.

The ayes appear to have it. The ayes have it, and the motion to report favorably is agreed to.

Without objection, the Chairman is authorized to move to go to conference pursuant to House rules. Without objection, the staff is directed to make any technical and conforming changes, and all Members will be given 2 days, as provided by House rules, in which to submit additional, dissenting, supplemental, or minority views.

○