President; but, in doing so, he literally healed the Nation. And I recall a very personal discussion with him one time where he said he knew full well that he would likely lose the election, because of the pardon, but he saw no alternative but to pardon President Nixon in order to put the whole Watergate episode behind us and get the Nation moving again.

I am privileged, and I have always felt a sense of honor, to be serving in the same House seat that Congressman Ford served. By publishing this book, we will educate future generations about the contributions of a great man who came from ordinary beginnings yet found himself performing well in extraordinary circumstances. Jerry Ford personified the many good traits that west Michigan has to offer our Nation, with his honesty, his forthrightness, and his hard work. And I urge my colleagues to support the creation of this commemorative volume. I urge strong support of this resolution.

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

Mr. BRADY of Pennsylvania. Mr. Speaker, I join my colleague from Michigan in support of this fitting tribute for our late President Ford. I urge the House to support the resolution.

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

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Pennsylvania (Mr. BRADY) that the House suspend the rules and agree to the concurrent resolution, H. Con. Res. 128.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the resolution was agreed to.

A motion to reconsider was laid on the table.

□ 1130

INTERNET SPYWARE (I-SPY) PREVENTION ACT OF 2007

Mr. CONYERS. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1525) to amend title 18, United States Code, to discourage spyware, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1525

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Internet Spyware (I–SPY) Prevention Act of 2007''.

SEC. 2. PENALTIES FOR CERTAIN UNAUTHORIZED ACTIVITIES RELATING TO COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Illicit indirect use of protected computers

''(a) Whoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and intentionally uses that program or code in furtherance of another Federal criminal offense shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) Whoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and by means of that program or code—

''(1) intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or

''(2) intentionally impairs the security protection of the protected computer with the intent to defraud or injure a person or damage a protected computer;

shall be fined under this title or imprisoned not more than 2 years, or both.

''(c) No person may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant's violating this section. For the purposes of this subsection, the term 'State' includes the District of Columbia, Puerto Rico, and any other territory or possession of the United States.

''(d) As used in this section—

''(1) the terms 'protected computer' and 'exceeds authorized access' have, respectively, the meanings given those terms in section 1030; and

''(2) the term 'personal information' means—

''(A) a first and last name;

''(B) a home or other physical address, including street name;

''(C) an electronic mail address;

''(D) a telephone number;

''(E) a Social Security number, tax identification number, drivers license number, passport number, or any other government-issued identification number; or

''(F) a credit card or bank account number or any password or access code associated with a credit card or bank account.

''(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following new item:

''1030A. Illicit indirect use of protected computers.''.

SEC. 3. AUTHORIZATION OF APPROPRIATIONS.

In addition to any other sums otherwise authorized to be appropriated for this purpose, there are authorized to be appropriated for each of fiscal years 2008 through 2011, the sum of $10,000,000 to the Attorney General for prosecutions needed to discourage the use of spyware and the practices commonly called phishing and pharming.

SEC. 4. FINDINGS AND SENSE OF CONGRESS CONCERNING THE ENFORCEMENT OF CERTAIN CYBERCRIMES.

(a) FINDINGS.—Congress makes the following findings:

(1) Software and electronic communications are increasingly being used by criminals to invade individuals' and businesses' computers without authorization.

(2) Two particularly egregious types of such schemes are the use of spyware and phishing scams.

(3) These schemes are often used to obtain personal information, such as bank account and credit card numbers, which can then be used as a means to commit other types of theft.

(4) In addition to the devastating damage that these heinous activities can inflict on individuals and businesses, they also undermine the confidence that citizens have in using the Internet.

(5) The continued development of innovative technologies in response to consumer demand is crucial in the fight against spyware.

(b) SENSE OF CONGRESS.—Because of the serious nature of these offenses, and the Internet's unique importance in the daily lives of citizens and in interstate commerce, it is the sense of Congress that the Department of Justice should use the amendments made by this Act, and all other available tools, vigorously to prosecute those who use spyware to commit crimes and those that conduct phishing and pharming scams.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Michigan (Mr. CONYERS) and the gentleman from Florida (Mr. KELLER) each will control 20 minutes.

The Chair recognizes the gentleman from Michigan.

Mr. CONYERS. Mr. Speaker, I yield myself as much time as I may consume.

Software and electronic communications are increasingly being used by criminals to invade individuals and businesses' computers without authorization. These practices undermine consumer confidence in the integrity and security of the Internet itself. Two particularly egregious examples involve the use of spyware and phishing scams.

Spyware is a form of software that helps gather information about an individual or organization without their knowledge. It also can be used to take control of someone else's computer and surreptitiously send information stored in that computer, such as the individual's personal information and passwords, to another entity where it can then be redirected for criminal purposes, including fraud, larceny, theft or other cybercrimes.

According to a survey last year by the FBI, computer security practitioners say that spyware is among the most critical threats to the security of our Nation's computer systems.

Phishing is another form of cybercrime. It is a scheme by which a criminal creates a Web site or sends e-mails that copy a well-known, legitimate business in an attempt to deceive Internet users into revealing personal information. Through phishing, for example, a criminal can trick an Internet user into revealing his bank account numbers or passwords.

Pharming is a version of phishing, and that involves the fraudulent use of domain names. In pharming, hijackers hijack a legitimate Web site's domain site and redirect traffic intended for the Web site to their own Web site where users may unknowingly provide personal information to the hacker.

This measure before us, H.R. 1525, aims to put a stop to these kinds of crimes that invade our privacy. It amends title 18 of the United States Code to impose criminal penalties, including up to 5 years in prison, on those who intentionally engage in spyware-related behavior in furtherance of other Federal criminal offenses.

Another thing the bill does is impose fines and imprisonment up to 2 years for anyone who engages in such practices with the intent to defraud or injure a person.

Finally, this measure authorizes $10 million per each fiscal year, 2008 through 2011, to help the Department of Justice combat these crimes.

I want to lift up the names of two of our Judiciary Committee members, Congresswoman ZOE LOFGREN of California, and of course, BOB GOODLATTE of Virginia, both of whom have put this legislation together and shepherded it through the hearing and the processes of the Judiciary Committee. I'd like to commend them for hard, effective work in developing and moving this bill on a bipartisan basis.

This is a targeted measure, ladies and gentlemen, that protects consumers by providing appropriately strong penalties for egregious behavior. I urge my colleagues to join us in support of it.

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

Mr. KELLER of Florida. Mr. Speaker, I yield myself as much time as I may consume.

Mr. Speaker, spyware is a serious and growing problem. This software allows criminals to hack into a computer to alter the user's security setting, collect personal information to steal a user's identity or commit other crimes.

H.R. 1525, the Internet Spyware Prevention Act of 2007, is bipartisan legislation that imposes criminal penalties on computer hacking intrusions and the use of spyware. A maximum term of 5 years imprisonment can be imposed for a hacking violation in which an unauthorized user accesses a computer.

In addition, a maximum of 2 years imprisonment can be imposed for anyone who uses spyware to break into a computer and alter the security settings or obtain the user's personal information.

This bill also authorizes $10 million for fiscal years 2008 through 2011 for the Department of Justice to increase Federal prosecutions of these new offenses.

I congratulate Congresswoman LOFGREN and Congressman GOODLATTE for their leadership and dedication on this issue. I also thank Chairman CONYERS and Crime Subcommittee Chairman SCOTT for their support of this legislation.

I urge my colleagues to vote ''yes'' on this bill, and I reserve the balance of my time.

Mr. CONYERS. Mr. Speaker, the gentlelady from California, ZOE LOFGREN, is the principal mover of this bill, and I'm pleased now to yield her as much time as she may consume.

Ms. ZOE LOFGREN of California. Mr. Speaker, I rise in support of H.R. 1525, the Internet Spyware Prevention Act of 2007. I'm very pleased that my first stand-alone bill that will be passed in this House under the new Democratic majority is one that both protects Americans on the Internet and fosters continued technological innovation. I thank my friend, Congressman BOB GOODLATTE, for working with me once again on this legislation to combat spyware.

Spyware is becoming one of the biggest threats to consumers on the Internet. Thieves are using spyware and key loggers are harvesting personal information from unsuspecting Americans. It also affects the business community that is forced to spend money to block and remove it from their systems.

Experts estimate that as many as 80 to 90 percent of all personal computers are infected with spyware. In short, it's a very real problem that's endangering consumers, damaging businesses and creating millions of dollars of additional costs.

This is a bipartisan measure that identifies the truly unscrupulous acts associated with spyware and subjects them to criminal punishment. This bill is the right approach because it focuses on behavior, not technology. It targets the worst forms of spyware without unduly burdening technological innovation.

The bill imposes tough criminal penalties on those who use spyware in furtherance of another Federal crime or to defraud or injure consumers. It also funds the Attorney General to find and prosecute spyware offenders and phishing scam artists.

Focusing on bad actors and criminal conduct is preferable to an approach that criminalizes technology or imposes notice-and-consent-type requirements. You know, bad actors don't comply with requirements. The more notices Internet users receive, in fact, the less likely they are to pay attention to any of them. Seventy-three percent of users don't read agreements, privacy statements or disclaimers on the Internet.

In 2005, the Pew Internet and American Life Project proved this point. A diagnostic site included a clause in one of its user agreements that promised $1,000 to the first person to write in and request the money. The agreement was downloaded more than 3,000 times before someone finally claimed the reward.

We don't want to overregulate user experience. We must avoid interfering with increasingly seamless, intuitive and interactive online environments. Regulation of technology is almost always a bad idea because technology changes faster than Congress can legislate; and what we attempt to regulate will morph into something else and render useless the regulatory scheme we adopt.

Legislation that attempts to control technology can also have the pernicious effect of chilling innovation by chilling investment into prohibited technological arenas. H.R. 1525 avoids these pitfalls by focusing on bad conduct, and that's why it has the broad support in my district in Silicon Valley, California.

What we're doing here today is important for consumers, for businesses. It's also important for the future of our high-tech economy.

I urge my colleagues on both sides of the aisle to vote in favor of this crucial legislation.

Mr. KELLER of Florida. Mr. Speaker, I yield as much time as he may consume to the gentleman from Virginia (Mr. GOODLATTE), who is the lead Republican cosponsor of this important legislation.

Mr. GOODLATTE. Mr. Speaker, I rise in strong support of H.R. 1525, the Internet Spyware or I–SPY Prevention Act.

I was pleased to join with my colleague from California, Representative ZOE LOFGREN, to reintroduce this legislation. This bipartisan bill will impose tough criminal penalties on those that use software for nefarious purposes without imposing a broad regulatory regime on legitimate online businesses. I believe that this targeted approach is the best way to combat spyware.

Spyware is software that provides a tool for criminals to secretly crack into computers to conduct nefarious activities such as altering a user's security settings, collecting personal information to steal a user's identity or to commit other crimes. A recent study done by the National Cybersecurity Alliance revealed that over 90 percent of consumers had some form of spyware on their computers, and most consumers were not aware of it.

The I–SPY Prevention Act would impose criminal penalties on the most egregious behavior associated with spyware. Specifically, this legislation would impose up to a 5-year prison sentence on anyone who uses software to intentionally break into a computer and uses that spyware in furtherance of another Federal crime.

In addition, it would impose up to a 2-year prison sentence on anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings or obtain personal information with the intent to defraud or injure a person, or with the intent to damage a computer. By imposing stiff penalties on these bad actors, this legislation will help deter the use of spyware and will thus help protect consumers from these aggressive attacks.

Enforcement is also crucial in combating spyware. The I–SPY Prevention Act authorizes $10 million for fiscal years 2008 through 2011 to be devoted to prosecutions involving spyware, phishing and pharming scams, and expresses the sense of Congress that the Department of Justice should vigorously enforce the laws against these crimes.

Phishing scams occur when criminals send fake e-mail messages to consumers on behalf of famous companies and request account information that is later used to conduct criminal activities.

Pharming scams occur when hackers redirect Internet traffic to fake sites in

order to steal personal information such as credit card numbers, passwords and account information.

This form of online fraud is particularly egregious because it is not as easily discernible by consumers. With pharming scams, innocent Internet users simply type the domain name into their Web browsers and the signal is rerouted to the devious Web site.

The I–SPY Prevention Act is a targeted approach that protects consumers by imposing stiff penalties on the truly bad actors, while protecting the ability of legitimate companies to develop new and exciting products and services online for consumers.

The I–SPY Prevention Act also avoids excessive regulation and its repercussions, including the increased likelihood that an overly regulatory approach focusing on technology would have unintended consequences that could discourage consumer use of the Internet, as well as the creation of new technologies and services on the Internet. By encouraging innovation, the I–SPY Prevention Act will help ensure that consumers have access to cutting-edge products and services at lower prices.

In addition, the approach of the I–SPY Prevention Act does not interfere with the free market principle that a business should be free to react to consumer demand by providing consumers with easy access to the Internet's wealth of information and convenience. Increasingly, consumers want a seamless interaction with the Internet, and we must be careful to not interfere with businesses' ability to respond to this consumer demand with innovative services. The I–SPY Prevention Act will help ensure that consumers, not the Federal Government, define what their interaction with the Internet looks like.

□ 1145

Finally, by going after the criminal behavior associated with the use of spyware, the I–SPY Prevention Act recognizes that not all software is spyware and that the crime does not lie in the technology itself but rather in actually using the technology for criminal purposes. People commit crimes; software doesn't.

H.R. 1525 is an effective, targeted approach to combating spyware, and I urge my colleagues to support this important legislation.

Mr. CONYERS. Mr. Speaker, I am now pleased to yield such time as he may consume to the chairman of the Subcommittee on Crime of the Judiciary Committee, the gentleman from Virginia, Mr. BOBBY SCOTT.

Mr. SCOTT of Virginia. I thank the chairman for yielding.

Mr. Speaker, I rise in support of H.R. 1525, the Internet Spyware (I–SPY) Prevention Act of 2007. I would like to commend Congresswoman LOFGREN and Congressman GOODLATTE for developing the legislation and moving the bill on a bipartisan basis. Earlier this month the Subcommittee on Crime, Terrorism, and Homeland Security held a hearing and markup on the bill and reported it favorably to the full committee.

The bill amends title 18, U.S. Code, to impose criminal penalties on those who use spyware to perpetrate identity theft and numerous other privacy intrusions on innocent Internet users. The bill also provides resources and guidance to the Department of Justice for the prosecution of these offenses.

The bill is narrowly aimed at the practices of using ''spyware'' and ''phishing'' to harm consumers. Recent studies estimate that 80 percent of computers are infected with some form of spyware and that 89 percent of consumers are unaware of the fact that they have spyware. The greatest security and privacy challenges posed by spyware relate to technologies such as keystroke logging programs that capture a user's passwords, Social Security, or account numbers. This information can then be redirected for criminal purposes including fraud, larceny, identity theft, or other cyber crimes.

This bill combats spyware by clarifying that it is a crime, punishable for up to 5 years in prison, to intentionally access a computer without authorization by causing a computer program or code to be copied onto a computer and then using that program or code in furtherance of another Federal criminal offense. The bill also provides fines or imprisonment up to 2 years for anyone who, through means of that program or code, intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person.

The bill also authorizes funds to combat ''phishing.'' Phishing is a general term for using what appears to others to be either the Web site of, or e-mails from, well-known, legitimate businesses in an attempt to deceive Internet users into revealing their personal information. Phishing is adequately covered by the criminal code under existing Federal wire fraud or identity theft statutes, but additional funds are needed to prosecute the crime. This bill would authorize $10 million for each of the fiscal years 2008–2011 to combat phishing and spyware.

I would also like to note that the Energy and Commerce Committee is considering a bill on this subject as well. But that bill lacks the criminal penalty enforcement mechanism in this bill and in its place imposes a regulatory scheme which focuses on the uses of technology rather than the perpetrators of crimes. My concern is such a regulatory regime may unavoidably sweep in legitimate uses of the technology.

The I–SPY Prevention Act is a strong bill that protects consumers by providing criminal penalties for egregious behavior. Accordingly, I urge my colleagues to support this legislation.

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

Mr. CONYERS. Mr. Speaker, this is a very important measure. We are finally dealing with those spyware crimes that invade our financial privacy, and I commend all of the actors on the Judiciary Committee that played a role in bringing this to our attention. Mr. RIC KELLER has done an excellent job as well.

Ms. JACKSON-LEE of Texas. Mr. Speaker, as a proud original co-sponsor of the legislation before us, I speak in strong support of H.R. 1525, the ''Internet Spyware (I–SPY) Prevention Act of 2007.''

H.R. 1525 amends the federal computer fraud and abuse statute to make it unlawful to access a computer without authorization or to intentionally exceed authorized access by causing a computer program or code to be copied onto the computer and using that program or code to transmit or obtain personal information (for example, first and last names, addresses, e-mail addresses, telephone numbers, Social Security numbers, drivers license numbers, or bank or credit account numbers).

Further, H.R. 1525 discourages the practice of phishing, another scourge of the Internet. ''Phishing'' is a general term for using what appears to be either the Web sites of, or e-mails that appear to be sent from, readily identifiable and legitimate businesses. These fraudulent Web sites and e-mails are designed to deceive Internet users into revealing personal information that can then be used to defraud those same users. The 'phishers' take that information and use it for criminal purposes, like identity theft and fraud. Phishing is adequately covered by the criminal code, but additional funds are needed to prosecute the crime. This bill would authorize 10 million dollars for each of the fiscal years 2008 to 2011 to combat phishing and spyware.

Mr. Speaker, as we all know too well, spyware is quickly becoming one of the biggest threats to consumers on the information superhighway. Spyware encompasses several potential risks, including the promotion of identity theft by harvesting personal information from consumer's computers. Additionally, it can adversely affect businesses, as they are forced to sustain costs to block and remove spyware from employees' computers, in addition to the potential impact on productivity.

Spyware has been defined as ''software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity with the consumer's consent, or asserts control over a computer with the consumer's knowledge.'' Among other things, criminals can use spyware to track every keystroke an individual makes, including credit card and social security numbers.

Some estimates suggest 25 percent of all personal computers contain some kind of spyware while other estimates show that spyware afflicts as many as 80–90 percent of all personal computers. Businesses are reporting several negative effects of spyware. Microsoft says evidence shows that spyware is ''at least partially responsible for approximately one-half of all application crashes'' reported to them, resulting in millions of dollars of unnecessary support calls.

The last point I wish to make, Mr. Speaker, is that H.R. 1525 is substantially similar to the bipartisan H.R. 744, introduced in the 109th Congress, which passed the House by a vote

of 395–1 and H.R. 4661, which passed the House during the 108th Congress by a vote of 415–0. H.R. 1525 is supported by numerous industry groups and privacy coalitions, including the Business Software Alliance, the Software & Information Industry Association, the U.S. Chamber of Commerce, and the Center for Democracy and Technology.

Mr. Speaker, I strongly support H.R. 1525 and urge all my colleagues to do likewise.

GENERAL LEAVE

Mr. CONYERS. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on the bill under consideration.

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

There was no objection.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Michigan (Mr. CONYERS) that the House suspend the rules and pass the bill, H.R. 1525, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

SECURING AIRCRAFT COCKPITS AGAINST LASERS ACT OF 2007

Mr. CONYERS. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1615) to amend title 18, United States Code, to provide penalties for aiming laser pointers at airplanes, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1615

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Securing Aircraft Cockpits Against Lasers Act of 2007''.

SEC. 2. PROHIBITION AGAINST AIMING A LASER POINTER AT AN AIRCRAFT.

(a) OFFENSE.—Chapter 2 of title 18, United States Code, is amended by adding at the end the following:

''§ 39A. Aiming a laser pointer at an aircraft

''(a) Whoever knowingly aims the beam of a laser pointer at an aircraft in the special aircraft jurisdiction of the United States, or at the flight path of such an aircraft, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) As used in this section, the term 'laser pointer' means any device designed or used to amplify electromagnetic radiation by stimulated emission that emits a beam designed to be used by the operator as a pointer or highlighter to indicate, mark, or identify a specific position, place, item, or object.

''(c) This section does not prohibit aiming a beam of a laser pointer at an aircraft, or the flight path of such an aircraft, by—

''(1) an authorized individual in the conduct of research and development or flight test operations conducted by an aircraft manufacturer, the Federal Aviation Administration, or any other person authorized by the Federal Aviation Administration to conduct such research and development or flight test operations;

''(2) members or elements of the Department of Defense or Department of Homeland Security acting in an official capacity for the purpose of research, development, operations, testing or training; or

''(3) by an individual using a laser emergency signaling device to send an emergency distress signal.

''(d) The Attorney General, in consultation with the Secretary of Transportation, may provide by regulation, after public notice and comment, such additional exceptions to this section, as may be necessary and appropriate. The Attorney General shall provide written notification of any proposed regulations under this section to the Committees on the Judiciary of the House and Senate, the Committee on Transportation and Infrastructure in the House, and the Committee on Commerce, Science and Transportation in the Senate not less than 90 days before such regulations become final.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 2 of title 18, United States Code, is amended by adding at the end the following new item:

''39A. Aiming a laser pointer at an aircraft.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Michigan (Mr. CONYERS) and the gentleman from Florida (Mr. KELLER) each will control 20 minutes.

The Chair recognizes the gentleman from Michigan.

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

Members of the House, when a laser is aimed at an aircraft cockpit, particularly at the critical stage of take-off or landing, it presents an imminent threat to aviation security and passenger safety. This has now been increasingly recognized, and we propose to do something about it today.

According to the Federal Aviation Administration, laser illuminations can temporarily disorient or even disable a pilot during critical stages of flight. And in some cases, a laser might also cause permanent physical injury to the pilot.

Since 1990 the FAA has reported more than 400 of these kinds of incidents. The rash of incidents involving laser beams is compounded by the concern that the low cost of hand-held laser devices could lead to even more incidents of these kinds happening in the future.

So the measure before us today responds to the problem by amending title 18 of our United States Code to impose criminal penalties on someone who knowingly aims a laser pointer at an aircraft or in its flight path within the special aircraft jurisdiction of the United States. The criminal penalties include imprisonment of up to 5 years and fines.

So I again extend a hand of thanks to Chairman BOBBY SCOTT of the Crime Subcommittee for expeditiously moving this bill forward. And I also commend the sponsor of this legislation, Ric Keller, who is floor manager today, the gentleman from Florida, for his leadership on addressing the danger that lasers can pose to aircraft.

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

Mr. KELLER of Florida. Mr. Speaker, I yield myself such time as I may consume.

Aiming a laser beam into the cockpit of an airplane is a clear and present danger to the safety of all those on board the aircraft.

This legislation is simple and straightforward. It makes it illegal to knowingly aim a laser pointer at an aircraft. Those who intentionally engage in such misconduct shall be fined or imprisoned not more than 5 years, or both, in the discretion of the judge.

This legislation was unanimously approved by all Republicans and Democrats on the House Judiciary Committee in this Congress and in the last Congress. It was also approved by the full House by a voice vote, and the Senate also approved this legislation by unanimous consent after slightly amending the legislation to provide for limited exceptions for testing and training by the Department of Defense and FAA, as well as using the laser to send an emergency distress signal. This bill represents the negotiated compromise between the House and Senate on these limited exceptions.

The problems caused by laser beam pranksters are more widespread than one might think. According to the FAA and the Congressional Research Service, there have been over 500 incidents reported since 1990 where pilots have been disoriented or temporarily blinded by laser exposure. The problem is on the rise, and there were over 90 incidents in 2005 alone.

These easily available laser pin pointers, like the one I purchased here at the Staples Office Supply Store for $12, have enough power to cause vision problems in pilots from a distance of 2 miles. It is only a matter of time before one of these laser beam pranksters ends up killing over 200 people in a commercial airline crash.

Surprisingly, there is currently no Federal statute on the books making it illegal to shine a laser beam into an aircraft cockpit, unless one attempts to use the PATRIOT Act to claim that the action was a ''terrorist attack or other attack of violence against a mass transportation system.''

So far none of the more than 500 incidents involving flight crew exposure to lasers have been linked to terrorism. Rather, it is often a case of pranksters making stupid choices to put pilots and their passengers at risk of dying. It is imperative that we send a message to the public that flight security is a serious issue. These acts of mischief will not be tolerated.

I wanted to learn what it was like to be in an aircraft cockpit hit by a laser beam; so I spoke with Lieutenant Barry Smith from my hometown of Orlando, Florida, who was actually in the cockpit of a helicopter that was hit by a laser beam.

Lieutenant Smith is with the Seminole County Sheriff's Office. He and his partner were in a police helicopter searching for burglary suspects at