....

(Original Signature of Member)

115TH CONGRESS
1ST SESSION

H. R. ______

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. GRAVES of Georgia introduced the following bill; which was referred to the Committee on ______________________________

A BILL

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

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 "Active Cyber Defense Certainty Act".

SEC. 2. CONGRESSIONAL FINDINGS.

Congress finds the following:

(1) Cyber fraud and related cyber-enabled crimes pose a severe threat to the national security and economic vitality of the United States.

(2) As a result of the unique nature of cybercrime, it is very difficult for law enforcement to respond to and prosecute cybercrime in a timely manner, leading to the existing low level of deterrence and a rapidly growing threat. In 2015, the Department of Justice prosecuted only 153 cases of computer fraud. Congress determines that this status quo is unacceptable and that if left unchecked, the trend in cybercrime will only continue to deteriorate.

(3) Cybercriminals have developed new tactics for monetizing the proceeds of their criminal acts, making it likely that the criminal activity will be further incentivized in the absence of reforms to current law allowing for new cyber tools and deterrence methods for defenders.

(4) When a citizen or United States business is victimized as the result of such crime, the first recourse should be to report the crime to law enforcement and seek to improve defensive measures.

(5) Congress also acknowledges that many cyberattacks could be prevented through improved cyber defensive practices, including enhanced training, strong passwords, and routine updating and patching to computer systems.

(6) Congress determines that the use of active cyber defense techniques, when properly applied, can also assist in improving defenses and deterring cybercrimes;

(7) Congress also acknowledges that many private entities are increasingly concerned with stemming the growth of dark web based cyber-enabled crimes. The Department of Justice should attempt to clarify the proper protocol for entities who are engaged in active cyber defense in the dark web so that these defenders can return private property such as intellectual property and financial records gathered inadvertently.

(8) Congress also recognizes that while Federal agencies will need to prioritize cyber incidents of national significance, there is the potential to assist the private sector by being more responsive to reports of crime through different reporting mechanisms. Many reported cybercrimes are not responded to in a time-

ly manner creating significant uncertainty for many businesses and individuals.

(9) Computer defenders should also exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside.

(10) Congress holds that active cyber defense techniques should only be used by qualified defenders with a high degree of confidence in attribution, and that extreme caution should be taken to avoid impacting intermediary computers or resulting in an escalatory cycle of cyber activity.

(11) It is the purposes of this act to provide legal certainty by clarifying the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network.

SEC. 3. EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY.

Section 1030 of title 18, United States Code, is amended by adding at the end the following:

"(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY.—

"(1) This section shall not apply with respect to the use of attributional technology in regard to a defender who uses a program, code, or command for attributional purposes that beacons or returns locational or attributional data in response to a cyber intrusion in order to identify the source of an intrusion; if—

"(A) the program, code, or command originated on the computer of the defender but is copied or removed by an unauthorized user; and

"(B) the program, code or command does not result in the destruction of data or result in an impairment of the essential operating functionality of the attacker's computer system, or intentionally create a backdoor enabling intrusive access into the attacker's computer system.

"(2) DEFINITION.—The term 'attributional data' means any digital information such as log files, text strings, time stamps, malware samples, identifiers such as user names and Internet Protocol addresses and metadata or other digital artifacts gathered through forensic analysis.".

SEC. 4. EXCLUSION FROM PROSECUTION FOR CERTAIN COMPUTER CRIMES FOR THOSE TAKING ACTIVE CYBER DEFENSE MEASURES.

Section 1030 of title 18, United States Code, is amended by adding at the end the following:

"(l) Active Cyber Defense Measures Not a Violation.—

"(1) Generally.—It is a defense to a criminal prosecution under this section that the conduct constituting the offense was an active cyber defense measure.

"(2) Inapplicability to civil action.—the defense against prosecution created by this section does not prevent a United States person or entity who is targeted by an active defense measure from seeking a civil remedy, including compensatory damages or injunctive relief pursuant to subsection (g).

"(3) Definitions.—In this subsection—

"(A) the term 'defender' means a person or an entity that is a victim of a persistent unauthorized intrusion of the individual entity's computer;

"(B) the term 'active cyber defense measure'—

"(i) means any measure—

"(I) undertaken by, or at the direction of, a defender; and

"(II) consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information in order to—

“(aa) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

“(bb) disrupt continued unauthorized activity against the defender’s own network; or

“(cc) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques; but

“(ii) does not include conduct that—

“(I) intentionally destroys or renders inoperable information that does not belong to the victim that is stored on another person or entity’s computer;

“(II) recklessly causes physical injury or financial loss as described under subsection (c)(4);

“(III) creates a threat to the public health or safety;

"(IV) intentionally exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

"(V) intentionally results in intrusive or remote access into an intermediary's computer;

"(VI) intentionally results in the persistent disruption to a person or entities internet connectivity resulting in damages defined under subsection (c)(4); or

"(VI) impacts any computer described under subsection (a)(1) regarding access to national security information, subsection (a)(3) regarding government computers, or to subsection (c)(4)(A)(i)(V) regarding a computer system used by or for a Government entity for the furtherance of the administration of justice, national defense, or national security;

"(C) the term 'attacker' means a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer; and

"(D) the term 'intermediary computer' means a person or entity's computer that is not under the ownership or primary control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack.".

SEC. 5. NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.

Section 1030 of title 18, Unites State Code, is amended by adding the following:

"(m) NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.—

"(1) GENERALLY.—A defender who uses an active cyber defense measure under the preceding section must notify the FBI National Cyber Investigative Joint Task Force and receive a response from the FBI acknowledging receipt of the notification prior to using the measure.

"(2) REQUIRED INFORMATION.—Notification must include the type of cyber breach that the person or entity was a victim of, the intended target of the active cyber defense measure, the steps the defender plans to take to preserve evidence of the attacker's criminal cyber intrusion, as well as the steps they plan to prevent damage to intermediary computers not under the ownership of the attacker and other information requested by the FBI to assist with oversight.".

SEC. 6. VOLUNTARY PREREEMPTIVE REVIEW OF ACTIVE CYBER DEFENSE MEASURES.

(a) PILOT PROGRAM.—The Federal Bureau of Investigation (hereinafter in this section referred to as the "FBI"), in coordination with other Federal agencies, shall create a pilot program to last for 2 years after the date of enactment of this Act, to allow for a voluntary preemptive review of active defense measures.

(b) ADVANCE REVIEW.—A defender who intends to prepare an active defense measure under section 4 may submit their notification to the FBI National Cyber Investigative Joint Task Force in advance of its use so that the FBI and other agencies can review the notification and provide its assessment on how the proposed active defense measure may be amended to better conform to Federal law, the terms of section 4, and improve the technical operation of the measure.

(c) PRIORITIZATION OF REQUESTS.—The FBI may decide how to prioritize the issuance of such guidance to defenders based on the availability of resources.

SEC. 7. ANNUAL REPORT ON THE FEDERAL GOVERNMENT'S PROGRESS IN DETERRING CYBER FRAUD AND CYBER-ENABLED CRIMES.

The Department of Justice, after consultation with the Department of Homeland Security and other relevant Federal agencies, shall deliver an annual report to Congress not later than March 31 of each year, detailing the results of law enforcement activities pertaining to cybercriminal deterrence for the previous calendar year. The report shall include—

(1) the number of computer fraud cases reported by United States citizens and United States businesses to FBI Field Offices, the Secret Service Electronic Crimes Task Force, The Internet Crimes Complaint Center (IC3) website, and other Federal law enforcement agencies;

(2) the number of investigations opened as a result of public reporting of computer fraud crimes, and the number of investigations open independently of any specific crimes being reported;

(3) the number of cyber fraud cases prosecuted under section 1030 of title 18, United States Code,

and other related statutes involving cybercrime, including the resolution of the cases;

(4) the number of computer fraud crimes determined to have originated from United States suspects and the number determined to have originated from foreign suspects, and details of the country of origin of the suspected foreign suspects;

(5) the number of dark web cybercriminal marketplaces and cybercriminal networks disabled by law enforcement activities;

(6) an estimate of the total financial damages suffered by United States citizens and businesses resulting from ransomware and other fraudulent cyber-attacks;

(7) the number of law enforcement personnel assigned to investigate and prosecute cybercrimes; and

(8) the number of active cyber defense notifications filed as required by this Act and a comprehensive evaluation of the notification process and voluntary preemptive review pilot program.

SEC. 8. REQUIREMENT FOR THE DEPARTMENT OF JUSTICE TO UPDATE THE MANUAL ON THE PROSECUTION OF CYBER CRIMES.

(a) The Department of Justice shall update the "Prosecuting Computer Crimes Manual," to reflect the changes made by this legislation.

(b) The Department of Justice is encouraged to seek additional opportunities to clarify the manual and other guidance to the public to reflect evolving defensive techniques and cyber technology that can be used in manner that does not violate section 1030 of title 18, United States Code, or other Federal law and international treaties.

SEC. 9. SUNSET.

The exclusion from prosecution created by this Act shall expire 2 years after the date of enactment of this Act.