

115TH CONGRESS
1ST SESSION

H. R. 4036

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

OCTOBER 12, 2017

Mr. GRAVES of Georgia (for himself and Ms. SINEMA) introduced the following bill; which was referred to the Committee on the Judiciary

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Active Cyber Defense
5 Certainty Act”.

6 **SEC. 2. CONGRESSIONAL FINDINGS.**

7 Congress finds the following:

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

4 (2) As a result of the unique nature of
5 cybercrime, it is very difficult for law enforcement to
6 respond to and prosecute cybercrime in a timely
7 manner, leading to the existing low level of deter-
8 rence and a rapidly growing threat. In 2015, the De-
9 partment of Justice prosecuted only 153 cases of
10 computer fraud. Congress determines that this sta-
11 tus quo is unacceptable and that if left unchecked,
12 the trend in cybercrime will only continue to deterio-
13 rate.

14 (3) Cybercriminals have developed new tactics
15 for monetizing the proceeds of their criminal acts,
16 making it likely that the criminal activity will be fur-
17 ther incentivized in the absence of reforms to cur-
18 rent law allowing for new cyber tools and deterrence
19 methods for defenders.

20 (4) When a citizen or United States business is
21 victimized as the result of such crime, the first re-
22 course should be to report the crime to law enforce-
23 ment and seek to improve defensive measures.

24 (5) Congress also acknowledges that many
25 cyberattacks could be prevented through improved

1 cyber defensive practices, including enhanced train-
2 ing, strong passwords, and routine updating and
3 patching to computer systems.

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

8 (7) Congress also acknowledges that many pri-
9 vate entities are increasingly concerned with stem-
10 ming the growth of dark web based cyber-enabled
11 crimes. The Department of Justice should attempt
12 to clarify the proper protocol for entities who are en-
13 gaged in active cyber defense in the dark web so
14 that these defenders can return private property
15 such as intellectual property and financial records
16 gathered inadvertently.

17 (8) Congress also recognizes that while Federal
18 agencies will need to prioritize cyber incidents of na-
19 tional significance, there is the potential to assist the
20 private sector by being more responsive to reports of
21 crime through different reporting mechanisms. Many
22 reported cybercrimes are not responded to in a time-
23 ly manner creating significant uncertainty for many
24 businesses and individuals.

1 (9) Computer defenders should also exercise ex-
2 treme caution to avoid violating the law of any other
3 nation where an attacker’s computer may reside.

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

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

14 **SEC. 3. EXCEPTION FOR THE USE OF ATTRIBUTIONAL**
15 **TECHNOLOGY.**

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

18 “(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL
19 TECHNOLOGY.—

20 “(1) This section shall not apply with respect to
21 the use of attributional technology in regard to a de-
22 fender who uses a program, code, or command for
23 attributional purposes that beacons or returns loca-
24 tional or attributional data in response to a cyber in-

1 intrusion in order to identify the source of an intru-
2 sion; if—

3 “(A) the program, code, or command origi-
4 nated on the computer of the defender but is
5 copied or removed by an unauthorized user; and

6 “(B) the program, code or command does
7 not result in the destruction of data or result
8 in an impairment of the essential operating
9 functionality of the attacker’s computer system,
10 or intentionally create a backdoor enabling in-
11 trusive access into the attacker’s computer sys-
12 tem.

13 “(2) DEFINITION.—The term ‘attributional
14 data’ means any digital information such as log files,
15 text strings, time stamps, malware samples, identi-
16 fiers such as user names and Internet Protocol ad-
17 dresses and metadata or other digital artifacts gath-
18 ered through forensic analysis.”.

19 **SEC. 4. EXCLUSION FROM PROSECUTION FOR CERTAIN**
20 **COMPUTER CRIMES FOR THOSE TAKING AC-**
21 **TIVE CYBER DEFENSE MEASURES.**

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

24 “(1) ACTIVE CYBER DEFENSE MEASURES NOT A
25 VIOLATION.—

1 “(1) GENERALLY.—It is a defense to a criminal
2 prosecution under this section that the conduct con-
3 stituting the offense was an active cyber defense
4 measure.

5 “(2) INAPPLICABILITY TO CIVIL ACTION.—the
6 defense against prosecution created by this section
7 does not prevent a United States person or entity
8 who is targeted by an active defense measure from
9 seeking a civil remedy, including compensatory dam-
10 ages or injunctive relief pursuant to subsection (g).

11 “(3) DEFINITIONS.—In this subsection—

12 “(A) the term ‘defender’ means a person
13 or an entity that is a victim of a persistent un-
14 authorized intrusion of the individual entity’s
15 computer;

16 “(B) the term ‘active cyber defense meas-
17 ure’—

18 “(i) means any measure—

19 “(I) undertaken by, or at the di-
20 rection of, a defender; and

21 “(II) consisting of accessing
22 without authorization the computer of
23 the attacker to the defender’s own
24 network to gather information in
25 order to—

1 “(aa) establish attribution of
2 criminal activity to share with
3 law enforcement and other
4 United States Government agen-
5 cies responsible for cybersecurity;

6 “(bb) disrupt continued un-
7 authorized activity against the
8 defender’s own network; or

9 “(cc) monitor the behavior
10 of an attacker to assist in devel-
11 oping future intrusion prevention
12 or cyber defense techniques; but

13 “(ii) does not include conduct that—

14 “(I) intentionally destroys or ren-
15 ders inoperable information that does
16 not belong to the victim that is stored
17 on another person or entity’s com-
18 puter;

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

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

24 “(IV) intentionally exceeds the
25 level of activity required to perform

1 reconnaissance on an intermediary
2 computer to allow for attribution of
3 the origin of the persistent cyber in-
4 trusion;

5 “(V) intentionally results in in-
6 trusive or remote access into an
7 intermediary’s computer;

8 “(VI) intentionally results in the
9 persistent disruption to a person or
10 entities internet connectivity resulting
11 in damages defined under subsection
12 (c)(4); or

13 “(VII) impacts any computer de-
14 scribed under subsection (a)(1) re-
15 garding access to national security in-
16 formation, subsection (a)(3) regarding
17 government computers, or to sub-
18 section (c)(4)(A)(i)(V) regarding a
19 computer system used by or for a
20 Government entity for the furtherance
21 of the administration of justice, na-
22 tional defense, or national security;

23 “(C) the term ‘attacker’ means a person or
24 an entity that is the source of the persistent un-

1 authorized intrusion into the victim’s computer;
2 and

3 “(D) the term ‘intermediary computer’
4 means a person or entity’s computer that is not
5 under the ownership or primary control of the
6 attacker but has been used to launch or obscure
7 the origin of the persistent cyber-attack.”.

8 **SEC. 5. NOTIFICATION REQUIREMENT FOR THE USE OF AC-**
9 **TIVE CYBER DEFENSE MEASURES.**

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

12 “(m) NOTIFICATION REQUIREMENT FOR THE USE
13 OF ACTIVE CYBER DEFENSE MEASURES.—

14 “(1) GENERALLY.—A defender who uses an ac-
15 tive cyber defense measure under the preceding sec-
16 tion must notify the FBI National Cyber Investiga-
17 tive Joint Task Force and receive a response from
18 the FBI acknowledging receipt of the notification
19 prior to using the measure.

20 “(2) REQUIRED INFORMATION.—Notification
21 must include the type of cyber breach that the per-
22 son or entity was a victim of, the intended target of
23 the active cyber defense measure, the steps the de-
24 fender plans to take to preserve evidence of the
25 attacker’s criminal cyber intrusion, as well as the

1 steps they plan to prevent damage to intermediary
2 computers not under the ownership of the attacker
3 and other information requested by the FBI to as-
4 sist with oversight.”.

5 **SEC. 6. VOLUNTARY PREEMPTIVE REVIEW OF ACTIVE**
6 **CYBER DEFENSE MEASURES.**

7 (a) **PILOT PROGRAM.**—The Federal Bureau of Inves-
8 tigation (hereinafter in this section referred to as the
9 “FBI”), in coordination with other Federal agencies, shall
10 create a pilot program to last for 2 years after the date
11 of enactment of this Act, to allow for a voluntary preemp-
12 tive review of active defense measures.

13 (b) **ADVANCE REVIEW.**—A defender who intends to
14 prepare an active defense measure under section 4 may
15 submit their notification to the FBI National Cyber Inves-
16 tigative Joint Task Force in advance of its use so that
17 the FBI and other agencies can review the notification and
18 provide its assessment on how the proposed active defense
19 measure may be amended to better conform to Federal
20 law, the terms of section 4, and improve the technical op-
21 eration of the measure.

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

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

4 The Department of Justice, after consultation with
5 the Department of Homeland Security and other relevant
6 Federal agencies, shall deliver an annual report to Con-
7 gress not later than March 31 of each year, detailing the
8 results of law enforcement activities pertaining to
9 cybercriminal deterrence for the previous calendar year.
10 The report shall include—

11 (1) the number of computer fraud cases re-
12 ported by United States citizens and United States
13 businesses to FBI Field Offices, the Secret Service
14 Electronic Crimes Task Force, the Internet Crimes
15 Complaint Center (IC3) website, and other Federal
16 law enforcement agencies;

17 (2) the number of investigations opened as a re-
18 sult of public reporting of computer fraud crimes,
19 and the number of investigations open independently
20 of any specific crimes being reported;

21 (3) the number of cyber fraud cases prosecuted
22 under section 1030 of title 18, United States Code,
23 and other related statutes involving cybercrime, in-
24 cluding the resolution of the cases;

25 (4) the number of computer fraud crimes deter-
26 mined to have originated from United States sus-

1 pects and the number determined to have originated
2 from foreign suspects, and details of the country of
3 origin of the suspected foreign suspects;

4 (5) the number of dark web cybercriminal mar-
5 ketplaces and cybercriminal networks disabled by
6 law enforcement activities;

7 (6) an estimate of the total financial damages
8 suffered by United States citizens and businesses re-
9 sulting from ransomware and other fraudulent
10 cyberattacks;

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

14 (8) the number of active cyber defense notifica-
15 tions filed as required by this Act and a comprehen-
16 sive evaluation of the notification process and vol-
17 untary preemptive review pilot program.

18 **SEC. 8. REQUIREMENT FOR THE DEPARTMENT OF JUSTICE**
19 **TO UPDATE THE MANUAL ON THE PROSECU-**
20 **TION OF CYBER CRIMES.**

21 (a) The Department of Justice shall update the
22 “Prosecuting Computer Crimes Manual” to reflect the
23 changes made by this legislation.

24 (b) The Department of Justice is encouraged to seek
25 additional opportunities to clarify the manual and other

1 guidance to the public to reflect evolving defensive tech-
2 niques and cyber technology that can be used in manner
3 that does not violate section 1030 of title 18, United
4 States Code, or other Federal law and international trea-
5 ties.

6 **SEC. 9. SUNSET.**

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

○