Cybersecurity: Cyber Crime Protection Security Act (S. 2111)—A Legal Analysis

Charles Doyle
Senior Specialist in American Public Law

March 12, 2012

Congressional Research Service
7-5700
www.crs.gov
R42403

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The Cyber Crime Protection Security Act (S. 2111) would enhance the criminal penalties for the cyber crimes outlawed in the Computer Fraud and Abuse Act (CFAA). Those offenses include espionage, hacking, fraud, destruction, password trafficking, and extortion committed against computers and computer networks. S. 2111 contains some of the enhancements approved by the Senate Judiciary Committee when it reported the Personal Data Privacy and Security Act (S. 1151), S.Rept. 112-91 (2011).

The bill would (1) establish a three-year mandatory minimum term of imprisonment for aggravated damage to a critical infrastructure computer; (2) streamline and increase the maximum penalties for the cyber crimes proscribed in CFAA; (3) authorize the confiscation of real property used to facilitate the commission of such cyber offenses and permit forfeiture of real and personal property generated by, or used to facilitate the commission of, such an offense, under either civil or criminal forfeiture procedures; (4) add such cyber crimes to the racketeering (RICO) predicate offense list, permitting some victims to sue for treble damages and attorneys' fees; (5) increase the types of password equivalents covered by the trafficking offense and the scope of federal jurisdiction over the crime; (6) confirm that conspiracies to commit one of the CFAA offenses carry the same penalties as the underlying crimes; and (7) provide that a cyber crime prosecution under CFAA could not be grounded exclusively on the failure to comply with a term of service agreement or similar breach of contract or agreement, apparently in response to prosecution theory espoused in *Drew*. With the exception of this last limitation on prosecutions, the Justice Department has endorsed the proposals found in S. 2111.

The bill has been placed on the Senate calendar. As of this date, S. 2111 has no House counterpart.

Related CRS reports include CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, available in abridged form as CRS Report RS20830, *Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*.

Contents

Tables

Contacts

Introduction

On February 15, 2012, Senator Leahy introduced the Cyber Crime Protection Act Security Act (S. 2111).[1] The bill, which was then placed on the calendar, is identical to some of the provisions of the Personal Data Privacy and Security Act of 2011 (S. 1151), approved by the Senate Judiciary Committee earlier.[2] It would amend several provisions of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, among other things. Numbered among its provisions are proposals to

- expand the type of CFAA violations that qualify as racketeering (RICO) predicate offenses;[3]
- increase the penalties for violations of CFAA;[4]
- adjust CFAA's password trafficking offense to protect a wider range of computers and password equivalents;[5]
- affirm that conspiring to commit a CFAA offense is punishable to the same extent as the underlying offense;[6]
- amend CFAA's forfeiture provisions to permit confiscation of real property used to facilitate a CFAA violation and to authorize civil forfeiture proceedings;[7]
- create a new offense for aggravated damage to a critical infrastructure computer, punishable by imprisonment for not less than three years nor more than 20 years;[8] and
- clarify CFAA's "unauthorized access" element.[9]

Both houses have held hearings in consideration of these and related proposals during this Congress.[10]

---

[1] 158 *Congressional Record* S699-702 (daily ed. February 15, 2012).

[2] S.Rept. 112-91 (2011). S. 2111's provisions correspond to sections 101, 103, 104, 105, 106, 109, and 110 in S. 1151, as reported.

[3] S. 2111, §2.

[4] S. 2111, §3.

[5] S. 2111, §4.

[6] S. 2111, §5.

[7] S. 2111, §6.

[8] S. 2111, §7.

[9] S. 2111, §8.

[10] *Cybersecurity: Evaluating the Administration's Proposal, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 112th Cong., 1st sess. (2011)(House Hearing I); *Cybersecurity: Protecting America's New Frontier, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 112th Cong., 1st sess. (2011)(House Hearing II); *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats, Hearing Before the Senate Comm. on the Judiciary*, 112th Cong., 1st sess. (2011)(Senate Hearing I); *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats, Hearing Before the Senate Comm. on the Judiciary*, 112th Cong., 1st sess. (2011)(Senate Hearing II); see also, *Cybersecurity: Innovative Solutions to Challenging Problems, Joint Hearing Before the Subcomm. on Intellectual Property, Competition and Internet and the Subcomm. on Crime, Terrorism and Homeland Security, of the House Comm. on the Judiciary*, 112th Cong., 1st sess. (2011)(Jt. House Hearing).

Background

Congress has been concerned with the threats posed by cyber crime since before enactment of CFAA.[11] It has amended CFAA regularly in order to keep pace with fast moving technological developments.[12] There are other laws that address the subject of crime and computers.[13] Other laws deal with computers as arenas for crime or as repositories of the evidence of crime or from some other perspective. CFAA, Section 1030, deals with computers as victims.

In its present form, Subsection 1030(a) outlaws seven distinct offenses:

- accessing a computer to commit espionage;[14]
- computer trespassing resulting in exposure to certain governmental, credit, financial, or computer-housed information;[15]
- computer trespassing in a government computer;[16]

[11] Congressional inquiry began no later than 1976, S. Comm. on Government Operations, *Problems Associated with Computer Technology in Federal Programs and Private Industry—Computer Abuses*, 94th Cong., 2d Sess. (1976) (Comm.Print). Hearings were held in successive Congresses thereafter until passage of the original version of the CFAA as part of the Comprehensive Crime Control Act of 1984, P.L. 98-473, 98 Stat. 2190; *see e.g.*, *Federal Computer Systems Protection Act: Hearings Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess.(1978); *S. 240, the Computer Systems Protection Act of 1979: Hearings Before the Subcomm. on Criminal Justice of the Senate Comm. on the Judiciary*, 96th Cong., 2d Sess.(1980); *Federal Computer System Protection Act, H.R. 3970: Hearings Before the House Comm. on the Judiciary*, 97th Cong., 2d Sess.(1982); *Computer Crime: Hearings Before the House Comm. on the Judiciary*, 98th Cong., 1st Sess. (1983).

[12] I.e., P.L. 99-474, §2, October 16, 1986, 100 Stat. 1213; P.L. 100-690, title VII, §7065, November 18, 1988, 102 Stat. 4404; P.L. 101-73, title IX, §962(a)(5), August 9, 1989, 103 Stat. 502; P.L. 101-647, title XII, §1205(e), title XXV, §2597(j), title XXXV, §3533, November 29, 1990, 104 Stat. 4831, 4910, 4925; P.L. 103-322, title XXIX, §290001(b)-(f), September 13, 1994, 108 Stat. 2097-2099; P.L. 104-294, title II, §201, title VI, Sec. 604(b)(36), October 11, 1996, 110 Stat. 3491, 3508; P.L. 107-56, title V, §506(a), title VIII, §814(a)-(e), October 26, 2001, 115 Stat. 366, 382-384; P.L. 107-273, div. B, title IV, §§4002(b)(1), (12), 4005(a)(3), (d)(3), November 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; P.L. 107-296, title II, §225(g), November 25, 2002, 116 Stat. 2158; P.L. 110-326, title II, §§203, 204(a), 205-208, September 26, 2008, 122 Stat. 3561, 3563.

[13] See generally, CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws,* from which portions of this report were borrowed.

[14] 18 U.S.C. 1030(a)(1)("(a) Whoever—(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it ... shall be punished as provided in subsection (c) of this section").

[15] 18 U.S.C. 1030(a)(2)("(a) Whoever ... (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains - (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer ... shall be punished as provided in subsection (c) of this section").

[16] 18 U.S.C. 1030(a)(3)("(a) Whoever ... (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively (continued...)

- committing fraud, an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce;[17]
- damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce;[18]
- trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce;[19] and
- threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[20]

Subsection 1030(b) makes it a crime to attempt or conspire to commit any of these offenses.[21] Subsection 1030(c) catalogs the penalties for committing the crimes described in Subsections 1030(a) and (b), penalties that range from imprisonment for not more than a year for simple cyberspace trespassing to imprisonment for life for damage to a computer system resulting in death. Subsection 1030(d) preserves the investigative authority of the Secret Service. Subsection 1030(e) supplies common definitions. Subsection 1030(f) disclaims any application to otherwise permissible law enforcement activities. Subsection 1030(g) creates a civil cause of action for victims of these crimes. Subsection 1030(h), which has since lapsed, required annual reports through 1999 from the Attorney General and Secretary of the Treasury on investigations under the damage paragraph (18 U.S.C. 1030(a)(5)).

Aggravated Damage of Infrastructure Computers

Section 7 of S. 2111 would outlaw aggravated damage of critical infrastructure computers: "It shall be unlawful to, during and in relation to a felony violation of section 1030, intentionally

(...continued)

for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States ... shall be punished as provided in subsection (c) of this section").

[17] 18 U.S.C. 1030(a)(4)("(a) Whoever ... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period ... shall be punished as provided in subsection (c) of this section").

[18] 18 U.S.C. 1030(a)(5)("(a) Whoever ... (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss ... shall be punished as provided in subsection (c) of this section").

[19] 18 U.S.C. 1030(a)(6)("(a) Whoever ... (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if - (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States ... shall be punished as provided in subsection (c) of this section").

[20] 18 U.S.C. 1030(a)(7)("(a) Whoever ... 18 U.S.C. 1030(a)(6)("(a) Whoever ... (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if - (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States ... shall be punished as provided in subsection (c) of this section").

[21] As will be discussed below, there may be some question whether conspiracy to violate any of the provisions of subsection 1030(a) may be prosecuted under subsection 1030(b) or only under the general conspiracy statute.

cause or attempt to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment—(1) of the operation of the critical infrastructure computer; or (2) of the critical infrastructure associated with the computer."[22] Although the new section creates a separate crime, the offense can be committed only in conjunction with a violation of CFAA, section 1030 ("... during and in relation to a felony violation of section 1030 ...").

Offenders would be required to serve a minimum of three years in prison and might be imprisoned for up to 20 years.[23] The new section would come with an array of provisions designed to block any effort to mitigate the impact of its mandatory minimum sentences. Thus, courts could not sentence offenders to probation, nor order the sentence to be served concurrent with any other sentence, nor reduce the sentence imposed for other offenses to account for the mandatory minimum.[24] Comparable restrictions attend the mandatory minimum sentencing provisions for aggravated identify theft.[25]

The new section's definition of "critical infrastructure computer" would be far reaching and appears to have been modeled after the definition in the terrorist training section.[26] It would cover public and private computer systems relating to matters "vital to national defense, national security, national economic security, [or] public health and safety."[27] Although the description would seem to extend to systems relating to electronic power generating and regional components of the critical infrastructure, the new section drops them from the list of examples found in the model.[28]

The section has no individual conspiracy element. Therefore, the section's 3-year mandatory minimum and 20-year maximum would not apply to conspiracy to violate the section. Instead, conspiracy to violate its proscriptions would be punishable under the general conspiracy statute, that is, by imprisonment for not more than 5 years.[29]

Statutes that establish a mandatory minimum sentence of imprisonment for commission of a federal crime are neither common nor rare. They are associated most often with capital offenses, drug offenses, firearms offenses, and sex offenses committed against children.[30] Critics claim that

[22] Proposed 18 U.S.C. 1030A(b).

[23] Proposed 18 U.S.C. 1030A(c).

[24] Proposed 18 U.S.C. 1030A(d). The court would be allowed to sentence an offender concurrently for multiple violations of the proposed section, 18 U.S.C. 1030A(d)(2), (4).

[25] 18 U.S.C. 1029A(b).

[26] 18 U.S.C. 2339D. A similar description appears in the U.S. Sentencing Guidelines, U.S.S.G. §5B1.1(b)(16), App. N. 13.

[27] 18 U.S.C. 2339D (items S. 2111 would add in bold; items it would drop in italics and brackets)(subparagraph designations omitted)("[T]the term 'critical infrastructure **computer**' means **a computer that manages or controls** systems and assets vital to national defense, national security, **national** economic security, public health or safety **or any combination of those matters, whether publicly or privately owned or operated,** including [*both regional and national infrastructure. Critical infrastructure may be publicly or privately owned; examples of critical infrastructure include*] gas and oil production, storage, or delivery systems, water supply systems, telecommunications networks, electrical power [*generation or*] delivery systems, financing and banking systems, emergency services [*(including medical, police, fire, and rescue services), and*] transportation systems and services [*(including highways, mass transit, airlines, and airports)*]; and government operations that provide essential services to the public").

[28] *Id*.

[29] 18 U.S.C. 371.

[30] See generally, CRS Report RL32040, *Federal Mandatory Minimum Sentencing Statutes*.

such statutes can lead to unduly harsh results and do little to contribute to sentencing certainty or the elimination of unwarranted sentencing disparity.[31] Proponents argue that they provide assurance that certain serious crimes are at least minimally and even handedly punished.[32]

Section 7's proposal is somewhat reminiscent of the mandatory minimum provisions of the aggravated identity theft statute, 18 U.S.C. 1028A.[33] Section 1028A sets a mandatory minimum sentence of two years imprisonment for anyone who engages in identity theft during and in relation to any of a series of predicate fraud offenses, or a minimum of five years if committed during or in relation to a federal crime of terrorism. In spite of the Sentencing Commission's traditional opposition to mandatory minimum sentencing statutes,[34] the Commission's most recent report on the subject was mildly laudatory of the identity theft provision.[35]

Administration officials have endorsed the mandatory minimums of Section 7 as an appropriate sanction and deterrent.[36] Some Members may remain to be convinced.[37]

Forfeiture

Property associated with a violation of CFAA is now subject to confiscation under criminal forfeiture procedures.[38] Criminal forfeiture procedures are conducted as part of a criminal prosecution and require conviction of the property owner.[39] Civil procedures are separate civil procedures conducted against the forfeitable property itself and require no conviction of the property owner.[40] In the case of property confiscated because it has facilitated the commission of an offense, criminal forfeiture may constitute punishment of an owner for using his property to commit the crime. Civil forfeiture may punish him for failing to prevent the use of his property to commit the crime.[41]

---

[31] Luna & Cassell, *Mandatory Minimalism*, 32 CARDOZO LAW REVIEW 1, 13 (2010)("A mandatory minimum deprives judges of the flexibility to tailor punishment to the particular facts of the case and can result in an unduly harsh sentence.... Inconsistent application of mandatory minimums has only exacerbated disparities, opponents argue, expanding the sentencing differentials in analogous cases"),

[32] *Id.* at 12("Mandatory minimums help eliminate these inequalities [attributable to judicial discretion], proponents argue, by providing uniformity and fairness for the defendants, certainty and predictability of outcomes, and higher level of integrity in sentencing").

[33] See generally, CRS Report R42100, *Mandatory Minimum Sentencing: Federal Aggravated Identity Theft*.

[34] United States Sentencing Commission, *Special Report to the Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System* (1991).

[35] United States Sentencing Commission, *Report to the Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System*, 369 (October 2011)("The problems associated with certain mandatory minimum penalties are not observed, or are not as pronounced, in identity theft offenses. The Commission believes this is due, in part, to 18 U.S.C. §1028A requiring a relatively short mandatory penalty and not requiring stacking of penalties for multiple counts. The statute is relatively new and is used in only a handful of districts, however, so specific findings are difficult to make at this time").

[36] Senate Hearing II, Prepared statement of Associate Deputy Att'y Gen. James A Baker, at 6-7.

[37] S.Rept. 112-91, at 9 (2011)("Chairman Leahy expressed concern that the mandatory minimum sentence would lead to unfair sentencing results, while not adding any deterrent value").

[38] 18 U.S.C. 1030(i), (j). For a general discussion of federal forfeiture law see, CRS Report 97-139, *Crime and Forfeiture*.

[39] F.R.Crim.P. 32.2; 18 U.S.C. 982.

[40] 18 U.S.C. 981, 983-984.

[41] Civil forfeitures may be either remedial, or punitive, or both. *Austin v. United States*, 509 U.S. 602, 618-19 (continued...)

The existing provisions call for criminal forfeiture of real and personal property derived from the proceeds of a CFAA violation and of personal property used to facilitate the offense. Section 6 would amend the provisions to permit confiscation of any real property used to facilitate the offense as well.[42] It would authorize the confiscation of real and personal property under civil forfeiture procedures, as well as under criminal procedures.[43]

There has been some objection that the proposal "would subject to forfeiture the house of the parents of a teenage hacker who has used a computer to attempt to break into someone's network if the parents were aware of this conduct."[44] This seems something of an overstatement. The innocent owner defense is available to a property owner who can prove that he was unaware of the misconduct that would otherwise require confiscation.[45] Yet, it is also available to a property owner who can establish that he "did all reasonably could be expected under the circumstances to terminate such use of the property."[46] For example, a property owner can be said to have done all he reasonably could, when he discloses the misconduct to authorities and in consultation with authorities takes action to prevent further misuse of his property.[47]

In addition, Section 6 of the bill would adjust the forfeiture provisions to account for the Supreme Court's interpretation of the word "proceeds" in another forfeiture statute. In *United States v. Santos*, the Justices declared that the word "proceeds" in the money laundering statute referred to profits of a money laundering predicate offense rather than the gross receipts generated by the predicate.[48] Presumably with *Santos* in mind, the section would amend the forfeiture provisions so that the "gross proceeds" of a CFAA violation would be subject to confiscation.[49]

Exceeds Authorized Access

An element of several of the crimes found in Subsection 1030(a) is the requirement that the defendant access the computer "without authorization" or that he "exceeds authorized access."[50]

(...continued)

(1993)("[F]orfeiture generally and statutory in rem forfeiture in particular historically have been understood, at least in part, as punishment.... These [innocent owner] exemptions serve to focus the provisions on the culpability of the owner in a way that makes them look more like punishment, not less.... The inclusion of innocent-owner defenses ... reveals a similar congressional intent to punish ...").

[42] Proposed 18 U.S.C. 1030(i), (j).

[43] *Id.*

[44] Jt. Hearing, Prepared statement of Leslie Harris, President and CEO of the Center for Democracy & Technology, at 15.

[45] 18 U.S.C. 983(d)(1), (2)(A)(i).

[46] 18 U.S.C. 983(d)(1), (2)(A)(ii).

[47] 18 U.S.C. 983(d)(2)(B)(i)("For the purposes of this paragraph, ways in which a person may show that such person did all that reasonably could be expected may include demonstrating that such person, to the extent permitted by law - (I) gave timely notice to an appropriate law enforcement agency of information that led the person to know the conduct giving rise to a forfeiture would occur or has occurred; and (II) in a timely fashion revoked or made a good faith attempt to revoke permission for those engaging in such conduct to use the property or took reasonable actions in consultation with a law enforcement agency to discourage or prevent the illegal use of the property").

[48] 553 U.S. 507, 524 (2008)(Scalia, J., with Justices Souter, Ginsburg, and Thomas, JJ.); *id*. at 528 (Stevens, J., concurring in the judgment).

[49] S.Rept. 112-91, at 9 (2011)("Section 6 amends 1030(i) and (j) to clarify the criminal forfeiture provision in section 1030 and to create a civil forfeiture provision to provide the procedures governing civil forfeiture").

[50] E.g., 18 U.S.C. 1030(a)(4)("Whoever ... (4) knowingly and with intent to defraud, accesses a protected computer (continued...)

By definition, a defendant "exceeds authorized access" when he gains authorized access but uses or alters information he is not authorized to use or alter.[51] The courts have experienced some difficulty applying the definition. There is some support for the proposition that the term allows an employee to use authorized access to his employer's computer for purposes other than those for which it was given, as long as the use was not contrary to explicit employer limitations.[52]

In *United States v. Drew*, the government brought a prosecution under Section 1030 based on the theory that the defendant exceeded authorized access to a social network, *MySpace*, when she violated the terms of the *MySpace* terms of service agreement by inaccurately identifying herself.[53] The court granted the defendant's motion for acquittal, because it considered the government's theory was too sweeping to avoid a vagueness challenge.[54]

Section 8 may have been drafted in response to *Drew*.[55] The section would amend the definition of the term "exceeds authorized access" to state:

> As used in this section ... (6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter*, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.*[56]

The purpose of the amendment would be "[t]o address civil liberties concerns about the scope of the Computer Fraud and Abuse Act" by amending it "to exclude from criminal liability conduct

---

(...continued)

without authorization, or exceeds authorized access ...").

[51] 18 U.S.C. 1030(e)(6).

[52] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1136 n.7 (9th Cir. 2009)("[N]othing in the CFAA suggests that a defendant's authorization to obtain information stored in a company computer is 'exceeded' if the defendant breaches a state law duty of loyalty to an employer ..."); *United States v. Nosal*, 642 F.3d 781, 782 (9th Cir. 2011), vac'd for rehearing en banc, 661 F.3d 1180 (9th Cir. 2011)("The government contends ... that an employee exceeds authorized access when he or she obtains information from the computer and uses it for a purposes that violates the employer's restrictions on the use of the information.... [W]e agree with the government"); *Pulte Homes, Inc. v. Laborers' Int'l Union,* 648 F.3d 295, 304 (6th Cir. 2011)("Under this definition [(18 U.S.C. 1030(e)(6))], an individual who is authorized to use a computer for certain purposes but goes beyond those limitations ... has exceeded authorized access").

[53] *United States v. Drew*, 259 F.R.D. 449, 461 (C.D.Cal. 2009).

[54] *Id.* at 467 (internal citations omitted)("Here, the Government's position is that the 'intentional' requirement is met simply by a conscious violation of a website's terms of service. The problem with that view is that it basically eliminates any limiting and/or guiding effect of the scienter element. It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publically available for access and use. However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered from the more serious (e.g. posting child pornography) to the more trivial (e.g. posting a picture of friends without their permission). All can be prosecuted. Given the 'standardless sweep' that results, federal law enforcement entities would be improperly free 'to pursue their personal predilections'").

[55] S.Rept. 112-91, at 9 ("During the Judiciary Committee hearing, several Members of the Committee, including the Chairman, raised concerns about the Justice Department's decision to bring criminal charges in *United States v. Lori Drew* ...").

[56] Proposed 18 U.S.C. 1030((e)(6)(language of the amendment in italics).

that exclusively involves a violation of a contractual obligation or agreement, such as an acceptable use policy, or terms of service agreement."

The Justice Department objected that the proposal would deter prosecution of inside cyber threats.[57] On the other hand, a second witness, a former Justice Department official, warned against the implications of the interpretation espoused in *Drew*.[58] The same witness implied that employment and other contractual disputes are more appropriately resolved through civil litigation rather than criminal prosecution.[59]

[57] S.Rept. 112-91, at 9-10 (2011)("In his testimony before the Committee, Associate Deputy Attorney General James Baker responded to concerns about the *Drew* prosecution by noting that the case was an anomaly. Specifically, Mr. Baker noted that if Congress responded to the *Drew* case by 'restricting the statute [by prohibiting claims bases solely upon a violation of terms of use or contractual agreements] ... [that] would make it difficult or impossible to deter and address serious insider threats through prosecution.' In addition, Mr. Baker cautioned against treating violations of contractual agreements in cyberspace any differently from violations of such agreements in other contexts. For example, he noted the fact that law enforcement can prosecute an employee who acts in violation of an office policy. Mr. Baker conceded that the Department of Justice would not appeal the court's decision to overturn the conviction in the Drew case").

[58] House Hearing II, Prepared statement of Prof. Orin S. Kerr, at 5-6: "As a practical matter, the key question has become whether conduct 'exceeds authorized access' merely because it violates a written restriction on computer access such as the Terms of Use of a website. The Justice Department has taken the position that it does. This interpretation has the effect of prohibiting an extraordinary amount of routine computer usage. It is common for computers and computer services to be governed by Terms of Use or Terms of Service that are written extraordinarily broadly. Companies write those conditions broadly in part to avoid civil liability if a user of the computer engages in wrongdoing. If Terms of Use are written to cover everything slightly bad about using a computer, the thinking goes, then the company can't be sued for wrongful conduct by an individual user. Those terms are not designed to carry the weight of criminal liability. As a result, the Justice Department's view that such written Terms should define criminal liability—thus delegating the scope of criminal law online to the drafting of Terms by computer owners—triggers a remarkable set of consequences. A few examples emphasize the point:

"(a) The Terms of Service of the popular Internet search engine Google.com says that '[y]ou may not use' Google if 'you are not of legal age to form a binding contract with Google.' The legal age of contract formation in most states is 18. As a result, a 17-year-old who conducts a Google search in the course of researching a term paper has likely violated Google's Terms of Service. According to the Justice Department's interpretation of the statute, he or she is a criminal.

"(b) The Terms of Use of the popular Internet dating site Match.com says that 'You will not provide inaccurate, misleading or false information ... to any other Member.' If a user writes in his profile that he goes to the gym every day—but in truth he goes only once a month—he has violated Match.com's Terms of Use. Similarly, a man who claims to be 5 foot 10 inches tall, but is only 5 foot 9 inches tall, has violated the Terms. So has a woman who claims to 32 years old but really is 33 years old. One study has suggested that about 80% of Internet dating profiles contain false or misleading information about height, weight and age alone. *See* John Hancock, et. al., *The Truth about Lying in Online Dating Profiles* (2007). If that estimate is correct, most Americans who have an Internet dating profiles are criminals under the Justice Department's interpretation of the CFAA.

"(c) Terms of Use can be arbitrary and even nonsensical. Anyone can set up a website and announce whatever Terms of Use they like. Perhaps the Terms of Use will declare that only registered Democrats can visit the website; or only people who have been to Alaska; or only people named 'Frank.' Under the Justice Department's interpretation of the statute, all of these Terms of Use can be criminally enforced. It is true that the statute requires that the exceeding of authorized access be 'intentional,' but this is a very modest requirement because the element itself is so easily satisfied. Presumably, any user who knows that the Terms of Use exist, and who intends to do the conduct that violated the Term of Use, will have 'intentionally' exceeded authorized access").

[59] *Id*. at 5 ("I do not see any serious argument why such conduct should be criminal. Computer owners and operators are free to place contractual restrictions on the use of their computers. If they believe that users have entered into a binding contract with them, and the users have violated the contract, the owners and operator scan sue in state court under a breach of contact theory. But breaching a contract should not be a federal crime").

Trafficking in Passwords

Section 4 would modify the wording of the password trafficking prohibition in 18 U.S.C. 1030(a)(6). The current version reads: "Whoever ... (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States."[60]

As amended, it would state: "Whoever ... (6) knowingly and with intent to defraud traffics (as defined in section 1029) in—(A) any password or similar information or means of access through which a protected computer as defined in subparagraphs (A) and (B) of subsection (e)(2) may be accessed without authorization; or (B) any means of access through which a protected computer as defined in subsection (e)(2)(A) may be accessed without authorization."[61]

The change would represent an expansion both in the coverage of password equivalents and in scope of federal jurisdiction. Paragraph (6) now simply refers to passwords and "similar information through which a computer may be accessed without authorization." The section would add to passwords and similar information, similar "means of access." The change was designed to clarify coverage of "other methods of confirming a user's identity, such as biometric data, single-use passcodes, or smart carts used to access an account."[62]

The section now applies when the victimized computer or computer system is that of the federal government or when the *trafficking* affects interstate or foreign commerce.[63] As amended, the section would apply when the victimized computer or computer system is that of the federal government or of a financial institution or when the *computer or computer system* is used in or affects interstate or foreign commerce.[64] The section would accomplish the change by using the existing definition of the term "protected computer."[65]

Racketeering Predicates

Section 2 would add violations of the Computer Fraud and Abuse Act to the RICO (Racketeer Influenced and Corrupt Organization) predicate offense list. Among other things, RICO outlaws conducting the affairs of an enterprise, which affects interstate commerce, through the patterned

[60] 18 U.S.C. 1030(a)(6).

[61] Proposed 18 U.S.C. 1030(a)(6).

[62] Senate Hearing II, Prepared statement of Associate Deputy Att'y Gen. James A. Baker, at 5; see also, House Hearing II, Prepared statement of Deputy Chief of the Computer Crime and Intellectual Property Section Richard W. Downing, at 5.

[63] 18 U.S.C. 1030(a)(6).

[64] Proposed 18 U.S.C. 1030(a)(6).

[65] 18 U.S.C. 1030(e)(2)("As used in this section ... (2) the term 'protected computer' means a computer—(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States").

commission of other criminal offenses (predicate offenses).[66] Adding a crime to the RICO predicate offense list has a number of law enforcement advantages—some obvious; some not so obvious. First, RICO offenses are punishable by imprisonment for not more than 20 years.[67] RICO predicate offenses are often less severely punished. Second, RICO authorizes the confiscation of property derived from a RICO violation.[68] Forfeiture is sometimes not a consequence of a crime that is not RICO predicate. Third, it provides a private cause of action with treble damages and attorneys' fees for the victims of a RICO violation.[69] Federal law only infrequently provides a federal cause of action for the benefit of victims of federal crimes that are not RICO predicates. Fourth, any RICO predicate offense is, by virtue of that fact alone, a money laundering predicate offense.[70] Federal money laundering statutes ban the use of the proceeds of a RICO predicate offense to promote further money laundering predicate offenses. And, they outlaw their use in any financial transaction involving more than $10,000. In both instances, RICO predicate offenses qualify as money laundering predicate offenses, even in the absence of other elements necessary for RICO prosecution.[71] Fifth, the proceeds involved in a money laundering offense are subject to confiscation, again without regard to whether a RICO violation can be shown.[72]

Not all of these law enforcement advantages would follow as consequence of Section 2, however. First, Section 1030(a)'s offenses are already money laundering predicates.[73] Consequently, no additional benefits in terms of a money laundering prosecution flow from adding Section 1030 to the RICO predicate offense list. Second, the espionage and certain of the damage offenses in Subsection 1030(a) are already somewhat obliquely listed as RICO predicate offenses. Any offense that falls within the definition of a federal crime of terrorism is a RICO predicate offense, regardless of whether it actually involves a crime committed for terrorist purposes.[74] The definition of a federal crime of terrorism includes violations of 18 U.S.C. 1030(a)(1)(espionage) and in some cases violations of 18 U.S.C. 1030(a)(5)(A) (intentional damage). Thus, for those violations, Section 2 holds new advantages. Third, Section 1030 already provides a private cause of action for some of the victims of a violation of the section,[75] although a RICO cause of action offers treble damages and attorneys' fees, while Section 1030 offers only compensatory damages.[76]

In summary, RICO violations are punished more severely than many of the violations of Section 1030, and the addition would "make it easier for the Government to prosecute certain organized criminal groups that engage in computer network attacks."[77] The change would also inure to the

[66] 18 U.S.C. 1962. See generally, CRS Report 96-950, *RICO: A Brief Sketch*.

[67] 18 U.S.C. 1963.

[68] *Id*.

[69] 18 U.S.C. 1964(c).

[70] 18 U.S.C. 1956(c)(7)(A), 1957(f)(3).

[71] 18 U.S.C. 1956, 1957.

[72] 18 U.S.C. 981(a)(1)(C).

[73] 18 U.S.C. 1956(c)(7)(D).

[74] 18 U.S.C. 1961(1)(G).

[75] 18 U.S.C. 1030(g).

[76] Compare 18 U.S.C. 1964(c) and 1030(g).

[77] S.Rept. 112-91, at 9 (2011).

benefit of those victims of Section 1030 violations who could take advantage of the RICO private cause of action provisions.

Nevertheless, some hearing witnesses questioned the wisdom of opening the civil RICO remedies to those who claim to be victims of CFAA offenses. They asserted that a business will often settle a meritless RICO suit (a) because of the taint associated with merely being accused of racketeering and (b) because of the risk of losing a suit involving treble damages and attorneys' fees under statute that is very broad and whose boundaries are sometimes unclear.[78]

Conspiracy

Subsection 1030(b) now declares that conspiracy or attempt to violate any of the Subsection 1030(a) offenses "shall be punished as provided subsection (c)," the subsection which sets the penalties for each of the CFAA substantive offenses.[79] Subsection (c), in turn, begins with an introductory statement that "[t]he punishment for an offense under subsection (a) or (b) of this section is," and proceeds to identify the penalties for each of the CFAA offenses and for attempting to commit each of those offenses in various subparagraphs.[80] For example, with respect to the penalty for fraud by a first time offender, Subsection (c) declares, "[t]he punishment for an offense under subsection (a) or (b) of this section is ... (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 attempt to commit an offense punishable under this subparagraph."[81] Neither subparagraph (3)(A) nor any of the other subparagraphs specifically mention conspiracy. Thus, Subsection (b) says conspiracy will be punished under Subsection (c) but Subsection (c) makes no mention of conspiracy per se. Reading conspiracy out of CFAA seems inconsistent with the wording of Subsection (b), but the actual wording of Subsection (c) affords that construction some support.

Changes elsewhere in the bill would magnify the impact of reading conspiracy out of CFAA. Under existing law, conspiracy to commit any federal felony is punishable by imprisonment for not more than five years.[82] The maximum for conspiracy to commit a misdemeanor is the maximum for the underlying misdemeanor.[83] Section 1030 in its present form punishes some violations as misdemeanors, some as five-year felonies, and some more severely. In the case of misdemeanors and five-year felonies, the maximum penalties are the same whether prosecution is under Section 1030 or under the general conspiracy statute. As noted in **Table 1** below, however,

[78] Jt. Hearing, Prepared statement of Leslie Harris, President and CEO of the Center for Democracy & Technology, at 15 ("Because of the vagueness of the law, making the CFAA a RICO predicate could have the unintended consequence of making legitimate businesses subject to civil RICO suits for routine and normal activities. While such lawsuits may be legally groundless, their reputational impact and the prospect of treble damages and attorneys fees will often drive legitimate businesses into settling unsustainable charges. Moreover, such lawsuits would intensify the feedback loop between civil and criminal law that has led to the current overbreadth on the criminal side: as civil plaintiffs, newly incentivized to sue under the CFAA, continue to take novel theories to court, the set of activities which are considered criminal will likely continue to expand"); *id*., Prepared statement of Robert W. Holleyman II on behalf of the Business Software Alliance, at 6.

[79] 18 U.S.C. 1030(b).

[80] E.g., 18 U.S.C. 1030(c).

[81] 18 U.S.C. 1030(c)(3)(A).

[82] 18 U.S.C. 371.

[83] *Id.*

Section 3 of the bill increases most of Subsection 1030(c)'s maximum penalties. Some of the subsection's misdemeanors (punishable by imprisonment for not more than one year) would become felonies (punishable by imprisonment for not more than three years). Some of its 5-year felonies would become 10- or 20-year felonies. In those instances, it would make a difference whether conspiracy could be prosecuted under Section 1030 with its corresponding penalties or would need to be prosecuted under the five-year general conspiracy statute.

Section 5 of the bill would address the issue by amending Subsection (b) of CFAA to read: "Whoever conspires to commit or attempt to commit an offense under subsection (a) of this section shall be punished as provided *for the completed offense* in subsection (c) of this section."[84]

Sentencing Increases

Section 3 would amend Subsection 1030(c) for a more streamlined statement of the penalties for the Subsection 1030(a) and 1030(b) offenses. In doing so, it would eliminate the penalty increases for repeat offenders. In many instances, it would set the penalties for all offenders at the levels now reserved for repeat offenders, and would punish novices and repeat offenders alike. One exception would be the maximum penalty available upon conviction under Subsection 1030(a)'s fraud provisions. There, the maximum penalty would be increased from 5 to 20 years.

Administration witnesses approved the general increases as a simplification of Subsection 1030(c) and as a means of affording federal judges the opportunity to punish more serious cyber offenses more severely.[85] In the case of the fraud increase, they explained that

> some of the CFAA's sentencing provisions no longer parallel the sentencing provisions of their equivalent traditional crimes. For example, the current maximum punishment for a violation of section 1030(a)(4) (computer hacking in furtherance of a crime of fraud) is five years, but the most analogous 'traditional' statutes, 18 U.S.C. §§1341 and 1343 (mail and wire fraud), both impose maximum penalties of twenty years.[86]

[84] Proposed 18 U.S.C. 1030(b)(language section 5 would add in italics).

[85] House Hearing II, Prepared statement of Deputy Chief of the Computer Crime and Intellectual Property Section Richard W. Downing, at 4-5; Senate Hearing II, Prepared statement of Associate Deputy Att'y gen. James A. Baker, at 4-5.

[86] House Hearing II, Prepared statement of Deputy Chief of the Computer Crime and Intellectual Property Section Richard W. Downing, at 5; Senate Hearing II, Prepared statement of Associate Deputy Att'y gen. James A. Baker, at 5.

Table 1. Sentences for Violations or Attempted Violations of 18 U.S.C. 1030

Maximum Term of Imprisonment

Existing Law	S. 2111, Section 3
Espionage: 10 years (20 years for repeat offenders), 18 U.S.C. 1030(c)(1)	20 years, proposed 18 U.S.C. 1030(c)(1)
Obtaining information by unauthorized access:	
(1)(a) committed for commercial or financial gain,	(1)(a) committed for commercial or financial gain,
(b) committed in furtherance of a criminal or tortious act, or	(b) committed in furtherance of a criminal or tortious act, or
(c) value of the information exceeds $5,000: 5 years, 18 U.S.C. 1030(c)(2)(B);	(c) value of the information exceeds $5,000: 10 years, proposed 18 U.S.C. 1030(c)(2)(B);
(2) repeat offenders: 10 years, 18 U.S.C. 1030(c)(2)(C);	
(3) otherwise: 1 year, 18 U.S.C. 1030(c)(2)(A)	(2) otherwise, 3 years, proposed 18 U.S.C. 1030(c)(2)(A)
Simple trespassing: 1 year (10 years for repeat offenders), 18 U.S.C. 1030(c)(2)(A), (C)	*1 year*, proposed 18 U.S.C. 1030(c)(3)
Unauthorized access with the intent to defraud: 5 years (10 years for repeat offenders), 18 U.S.C. 1030(c)(3)	20 years, proposed 18 U.S.C. 1030(c)(4)
Causing damage:	
(1) intentionally: (a) knowingly or recklessly causing death: any term of years or life, 18 U.S.C. 1030(c)(4)(F)	(1) intentionally: (a) knowingly or recklessly causing death: any term of years or life, proposed 18 U.S.C. 1030(c)(5)(C)
(b) knowingly or recklessly causing serious bodily injury: 20 years, 18 U.S.C. 1030(c)(4)(E)	no comparable provision
(c)(i) causing at least $5,000 in losses, (ii) involving medical treatment, (iii) causing physical injury, (iv) causing a threat to public safety, (v) damage affecting a U.S. law enforcement, national security, or national defense computer, (vi) affecting 10 or more protected computers: 10 years (20 years for repeat offenders), 18 U.S.C. 1030(c)(4)(B), (C)	(b)(i) causing at least $5,000 in losses, (ii) involving medical treatment, (iii) causing physical injury, (iv) causing a threat to public safety, (v) damage affecting a U.S. law enforcement, national security, or national defense computer, (vi) affecting 10 or more protected computers: 20 years, proposed 18 U.S.C. 1030(c)(5)(A)
(2) recklessly:)(i) causing at least $5,000 in losses, (ii) involving medical treatment, (iii) causing physical injury, (iv) causing a threat to public safety, (v) damage affecting a U.S. law enforcement, national security, or national defense computer, (vi) affecting 10 or more protected computers: 5 years (20 years for repeat offenders), 18 U.S.C. 1030(c)(4)(A), (C)	(2) recklessly:)(i) causing at least $5,000 in losses, (ii) involving medical treatment, (iii) causing physical injury, (iv) causing a threat to public safety, (v) damage affecting a U.S. law enforcement, national security, or national defense computer, (vi) affecting 10 or more protected computers: 10 years, proposed 18 U.S.C. 1030(c)(5)(B)
(3) causing loss: 10 years for repeat offenders, 18 U.S.C. 1030(c)(4)(D)	no comparable provision
(4) otherwise: 1 year, 18 U.S.C. 1030(c)(4)(G)	(3) otherwise: 1 year, proposed 18 U.S.C. 1030(c)(5)(D)
Traffic in passwords: 1 year (10 years for repeat offenders), 18 U.S.C. 1030(c)(2)(A), (C)	10 years, proposed 18 U.S.C. 1030(c)(6)
Extortion: 5 years (10 years for repeat offenders), 18 U.S.C. 1030(c)(3)	10 years, proposed 18 U.S.C. 1030(c)(7)

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968