The Obama Administration's Cybersecurity Proposal: Criminal Provisions

Gina Stevens
Legislative Attorney

Jonathan Miller
Legal Intern

July 29, 2011

Congressional Research Service
7-5700
www.crs.gov
R41941

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Responding to ongoing concerns over the state of U.S. cybersecurity, the Obama Administration released a report containing a proposal for significant cybersecurity legislation on May 12, 2011. The Administration's proposal contains seven sections and addresses many different subject areas. This report examines the first section of the Administration's proposal, dealing with criminal law. That section would supplement the Computer Fraud and Abuse Act (CFAA) by adding a mandatory three-year minimum penalty for damaging certain critical infrastructure computers, increase the penalties for most violations of the CFAA, modify the conspiracy and forfeiture provisions of the CFAA, and make felony violation of the CFAA a racketeering predicate offense.

This report also compares the Administration's proposal to bills pending before the House of Representatives and the Senate. Although Congress is considering many bills addressing cybersecurity, there are relatively few which would modify computer crime laws such as the CFAA. The bills which do address computer crime differ in significant ways from the Administration's proposal, though they would accomplish some of the same goals.

Contents

Contacts

Background[1]

Over the past decade, cybersecurity has become a steadily more important issue in Washington. President Clinton recognized computer networks and information systems as critical infrastructure in 1998.[2] By 2003, President Bush acknowledged that critical infrastructure, including computer networks, was vulnerable to attack and that security improvements were needed.[3] In August 2007, the Center for Strategic and International Studies (CSIS) formed a commission to evaluate U.S. cybersecurity policy and to make recommendations for improving that policy. The commission's report highlighted the vulnerability of the United States to cyberattacks and made seven broad policy recommendations to address weaknesses in U.S. cyberdefenses. One of the commission's findings was that U.S. computer crime laws are decades old, written for a less connected era, and insufficient to confront modern challenges.[4] Additionally, the commission found that criminals and foreign intelligence services operating on the Internet pose a serious danger to the economic and national security interests of the United States.[5] The report claims that "a complex interchange of definitions, prohibitions, and permissions," built up over decades, has resulted in unnecessary legal complexity.[6] To address this problem, the report recommends modernizing legal authorities, including criminal statutes, to increase clarity, speed investigations, and better protect privacy.[7]

Upon taking office, President Obama commissioned a 60-day cyberspace policy review. The review underscored the seriousness of the cybersecurity problem, saying that "the growing connectivity between information systems, the Internet, and other infrastructure creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."[8] Additionally, the review focused on the potential for computer hackers to disrupt U.S. critical infrastructure and the growth of criminal activity online.[9]

In response to congressional calls for comprehensive cybersecurity legislation the Obama Administration released a legislative cybersecurity proposal on May 12, 2011.[10] The

---

[1] This report was prepared by Jonathan H. Miller, Legal Intern, American Law Division, under the general supervision of Gina Stevens, Legislative Attorney.

[2] Presidential Decision Directive 63 (1998) available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[3] *See* Homeland Security Presidential Directive 7 (2003) available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[4] *See* Securing Cyberspace for the 44th Presidency 2 (Center for Strategic and International Studies, 2008) available at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[5] *Id.* at 3.

[6] *Id.* at 67.

[7] *Id.* at 8.

[8] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure 1 (2009) available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (quoting the Director of National Intelligence).

[9] *Id.* at 2.

[10] *See* Letter from Harry Reid, Sen. Maj. Leader, to Barack Obama, President (July 1, 2010) (http://www.govexec.com/pdfs/070210cr1.pdf); Office of Management and Budget, Complete Cybersecurity Proposal (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

Administration's proposal contains seven sections and addresses many different subject areas. The proposal includes sections on criminal law, national data breach notification, the Department of Homeland Security's cybersecurity authority, information sharing with the private sector, the regulatory framework covering critical infrastructure, coordination of federal information security policy, hiring cybersecurity experts, and the location of data centers. The Administration's proposal would address concerns raised in earlier reports by modifying the Computer Fraud and Abuse Act (CFAA).[11] The proposal implements a recommendation of the CSIS report by simplifying the complex penalty provisions of the CFAA. It also addresses a concern of the 60-day cybersecurity policy review by enhancing criminal penalties for damaging U.S. critical infrastructure. Overall, the proposal would

- supplement the CFAA with a mandatory minimum penalty for damaging certain critical infrastructure computers;
- increase the penalties for most violations of the CFAA;
- modify the conspiracy and forfeiture provisions of the CFAA;
- and make felony violation of the CFAA a racketeering predicate offense.

Protecting Critical Infrastructure Computers

Federal courts have interpreted the Computer Fraud and Abuse Act to include critical infrastructure within the definition of a protected computer.[12] Furthermore, the U.S. Sentencing Guidelines Manual includes sentence enhancements for violations of the CFAA involving a computer system used to maintain or operate critical infrastructure.[13] The sentencing guidelines are advisory only and do not create a minimum sentence.[14]

The Obama Administration's cybersecurity proposal would add a specific provision imposing a mandatory three-year term of imprisonment for damaging certain critical infrastructure computers.[15] A critical infrastructure computer is a computer, under this broad definition, which controls systems vital to national defense, national security, national economic security, or public health and safety. The critical infrastructure computer may be owned or operated by the government or privately. The proposal specifies that the term covers, at least, computers engaged in oil and gas production, water supply systems, telecommunications networks, electrical power systems, banking systems, emergency services, and transportation systems. For example, gaining unauthorized access to a radio system used at a private company to control oil production would likely qualify as a violation under the proposal.

[11] 18 U.S.C. § 1030; *See generally* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

[12] *See* United States v. Mitra, 405 F.3d 492 (7th Cir. Wis. 2005) (in which a computer hacker's conviction for interfering with a city emergency communications system was upheld).

[13] U.S. Sentencing Guidelines Manual § 2B1.1 (B)(16).

[14] *See* United States v. Booker, 543 U.S. 220 (2005).

[15] Office of Management and Budget, Law Enforcement Provisions Related to Computer Security (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security.pdf [hereinafter OMB, Provisions].

The proposal's definition of computer is the same as the one provided in the CFAA, namely "an electronic, magnetic optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions." Under the CFFA, a "computer" is not just a desktop or laptop but includes cellular phones[16] and radios.[17] The definition is broad and captures any device that makes use of an electronic data processor.[18]

The Administration's intention is to create a mandatory minimum sentence for violations of the CFAA which threaten critical infrastructure. The proposal seeks to ensure that courts impose a sufficiently deterrent sentence in the event of an attack on a critical infrastructure system, even a minor or unsuccessful attack.[19] The proposal would add a three-year term of imprisonment for damage to a critical infrastructure computer which occurred during a felony violation of the CFAA. In order to qualify, the damage must substantially impair the operation of the critical infrastructure computer or the critical infrastructure associated with the computer.

The proposal also attempts to ensure that felons who merit the additional three-year term of imprisonment serve the full term. The proposal has language, patterned on the mandatory sentencing provision for aggravated identity theft, which prohibits probation and concurrent terms of imprisonment in most cases.[20] This language would create a mandatory minimum sentence of three years for damaging a critical infrastructure computer in violation of the CFAA. Under the proposal, the court would have some discretion to impose a concurrent sentence but only for an additional violation of the new section sentenced at the same time.

Clarifying and Enhancing Penalties Under the Computer Fraud and Abuse Act

The Administration's proposal modifies many of the penalty provisions in the CFAA, in the process creating the possibility of longer sentences. Currently, the CFAA takes a two-tiered approach to penalties.[21] Penalties for violations of the act are set at one level for a first offense and then enhanced for subsequent violations of the statute. For example, the maximum penalty for stealing national defense information through unauthorized access to a computer is currently 10 years for the first offense and 20 years for a subsequent offense. The Administration's proposal

[16] *See* United States v. Kramer, 631 F.3d 900 (8th Cir. 2011) (holding that under the CFAA the term computer includes a cellular telephone).

[17] *See Mitra* at 495 (finding interference with a computer-based radio system a violation of the CFAA).

[18] *Kramer* at 902; *accord* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1577 (2010) ("Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of 'computer.' That category can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers." (footnote omitted)).

[19] *See* Office of Management and Budget, Law Enforcement Provisions Related to Computer Security, Section by Section Analysis (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Section-By-Section-Analysis.pdf [hereinafter OMB, Section Analysis].

[20] 18 U.S.C. § 1028A(b) (discussing sentencing for aggravated identity theft); *see also* OMB, Section Analysis, *supra* note 19.

[21] 18 U.S.C. § 1030(c)(2) – (4); *see generally*, Charles Doyle, (CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, 2010).

would simplify this two-tiered system by removing references to subsequent convictions in favor of setting a maximum sentence for each offense. In general, the maximum would be the number of years currently designated for a second offense.[22] Continuing the earlier example, the maximum penalty for stealing national defense information through unauthorized access to a computer would be 20 years under the proposal.

The proposal would also amend the password trafficking provision of the CFAA, which prohibits transferring password information to another when the information could be used to access a government computer or affects interstate commerce. The change would broaden the scope of the provision to cover any protected computer, removing the requirement that the trafficking affect interstate commerce or that the password be to a computer used by the government. The proposal would also expand the provision to protect means of access other than simply passwords. Critics have pointed out that this change may unintentionally criminalize consumers' otherwise lawful modification of electronic devices.[23] Supporters believe the provision is necessary to modernize the law in a world where passwords are not the only means of controlling access to information.[24]

The Administration's proposal would also modify the conspiracy portion of the CFAA. Currently, the law states that "whoever conspires to commit or attempts to commit an offense under [the CFAA] shall be punished as provided for in [the penalties subsection.]"[25] Although the penalty subsection makes explicit reference to violations of the CFAA and attempts to commit them, it does not mention conspiracy specifically. The proposal clarifies any ambiguity by stating that "Whoever conspires to commit ... an offense ... shall be punished as provided for the completed offense."[26]

Beyond simplification and clarification, the proposal seeks to increase the deterrent effect of the CFAA by increasing sentence length.[27] The Administration feels that the proposal would harmonize the penalties in the CFAA with other similar laws, such as the laws covering wire fraud.[28] Critics suggest that the definitions in the CFAA are too broad and should be more focused before penalties are enhanced.[29] Some critics argue that recent court cases enlarging the definition of unauthorized access should be addressed first.[30] Specifically, critics point to a recent Ninth

[22] OMB, Section Analysis, *supra* note 19.

[23] *See* Joshua Gruenspecht, *WH Cybersecurity Proposal: CFAA Hack Goes Beyond Hackers*, Center for Democracy and Technology (July 22, 4:30 PM), http://cdt.org/blogs/joshua-gruenspecht/wh-cybersecurity-proposal-cfaa-hack-goes-beyond-hackers.

[24] *See* Cybersecurity: Innovative Solutions to Challenging Problems, Before the H. Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 46 (2011) (Testimony of Leigh Williams, President, BITS).

[25] 18 U.S.C. § 1030(b).

[26] OMB, Provisions, *supra* note 15.

[27] *See id.*

[28] Cybersecurity: Innovative Solutions to Challenging Problems, Before the H. Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 7 (2011) (Statement of James Baker, Assoc. Deputy Att'y General, U.S. Dep't. of Justice); *but see* 18 U.S.C. 2701, 2511 (the significantly different penalties for violation of the arguably more analogous Electronic Communications Privacy Act).

[29] Cybersecurity: Innovative Solutions to Challenging Problems, Before the H. Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 56-57 (2011) (Statement of Leslie Harris, President, Center for Democracy and Technology).

[30] Joshua Gruenspecht, *WH Cybersecurity Proposal: CFAA Hack Goes Beyond Hackers*, Center for Democracy and Technology (July 22, 4:30 PM), http://cdt.org/blogs/joshua-gruenspecht/wh-cybersecurity-proposal-cfaa-hack-goes-beyond-hackers.

Circuit decision holding that violation of an employer's computer-use restrictions constitutes a criminal violation of the CFAA.[31] Critics also point to the highly publicized cyber-bullying trial of Lori Drew for violation of the MySpace terms of service as a troubling expansion of "unauthorized access" under the CFAA.[32] There is also concern from some that mandatory minimums and enhanced sentences could be too stringent for adolescent computer mischief, and that the Administration's proposal does not have sufficient flexibility to account for such crimes.[33]

Finally, the Administration's proposal would update the criminal forfeiture provision of the CFAA and add a civil forfeiture provision. Whereas criminal forfeiture results from the conviction of the property owner, civil forfeiture is conducted against the property itself. No conviction or charge against the property owner is required in the case of civil forfeiture. Both provisions would be amended to include real property, in addition to personal property, that facilitated the commission of the underlying offense.[34] The proposal would also establish a comparable civil forfeiture procedure by adding the CFAA to the list of racketeering predicates.[35] Additionally, both provisions would be modified to clarify that the government could seize any property resulting from gross proceeds of the violation as opposed to net proceeds. This expands the forfeiture provisions to cover property bought by money obtained from violating the CFAA. The civil forfeiture proceedings would be governed by the preexisting federal law on civil forfeitures.[36] However, the civil forfeitures would be overseen by the Secretary of Homeland Security or the Attorney General instead of the Secretary of the Treasury.

Addition of Computer Crime to RICO

Currently, violation of the CFAA is not a predicate offense under the Racketeering Influenced and Corrupt Organizations Act (RICO) in most instances.[37] The Administration's proposal would add violation of the CFAA to the list of predicate offenses chargeable under RICO. This addition would not change the scope of the CFAA, but it would enlarge the civil and criminal consequences for its violation. It would condemn any person who invests in, maintains an interest in, or conducts or participates in the affairs of an enterprise which engages in a patterned violation of the CFAA.[38] A patterned violation of the CFAA means two or more violations of the act that have the same or similar purpose and occur over a period of time.

Additionally, adding the CFAA to the list of predicate offenses would enhance the government's ability to prosecute computer crime conspiracy. Under RICO, a conspiracy is complete upon the

[31] *See* United States v. Nosal, 642 F.3d 781 (9th Cir. Cal. 2011).

[32] *See* U.S. v. Lori Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (holding that a violation of a website's terms of service, without more, is insufficient to constitute violation of the CFAA).

[33] Cybersecurity: Innovative Solutions to Challenging Problems, Before the H. Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 4 (2011) (Statement of Rep. Mel Watt, Ranking Member, H. Subcomm. on Intellectual Property, Competition, and the Internet).

[34] *Compare* 18 U.S.C. § 981(a)(1)(C) (which authorizes civil forfeiture of real or personal property derived from proceeds traceable to violation of the CFAA, as opposed to the broader property that facilitated the violation).

[35] 18 U.S.C. § 981(a)(1)(C) (civil forfeiture traceable to money derived from money laundering); 18 U.S.C. § 1956(c)(7)(A) (any RICO predicate is also a money laundering predicate).

[36] *See* 18 U.S.C. § 981 *et seq.*

[37] *See* 18 U.S.C. § 1961-68; *see generally* CRS Report 96-950, *RICO: A Brief Sketch*, by Charles Doyle.

[38] *See* 18 U.S.C. § 1962.

agreement to commit a violation of the act, even if no conspirator ever commits an overt act toward accomplishing that purpose.[39] Because there is no requirement to prove an overt act in furtherance of the conspiracy, RICO conspiracy is easier to prove.

A RICO violation is punishable by a fine or up to 20 years in prison. RICO violations may result in civil, as well as criminal liability. Any person injured in business or property by reason of a RICO violation has a cause of action for treble damages and attorneys' fees. In most cases, no prior criminal conviction is required to sue for civil damages.[40]

Comparison to Pending Legislation

There are currently many different bills pending before the House and Senate which grapple with cybersecurity issues. Few of these bills directly address the same criminal statutes as the Obama Administration's proposal. However, there is significant overlap between pending legislation and other provisions of the proposal. As of this writing, two Senate bills would update the CFAA to address modern challenges to cybersecurity. Both bills take a different approach than the one taken by the Administration's cybersecurity proposal, though both aim to accomplish some of the same objectives.

Personal Data Privacy and Security Act of 2011

The Personal Data Privacy and Security Act of 2011 (S. 1151), introduced by Senator Patrick Leahy on June 7, 2011, amends both RICO and the CFAA. Both S. 1151 and the Administration's proposal add felony violation of the CFAA to the list of predicate offenses under RICO.[41] Although the bill and the proposal have slightly different language, their effect on the RICO statute would appear to be identical. S. 1151 also amends the penalty provisions of the CFAA, though not so extensively as the Administration's proposal.[42] The bill aims to clarify the penalty for conspiracy to violate the CFAA by appending conspiracy to the various penalty provisions of the CFAA.[43] Unlike the Administration's proposal, the bill does not include unequivocal language stating that a conspiracy to violate the CFAA should be punished as if the underlying crime occurred. Additionally, the bill does not enhance penalties for violation of the CFAA, as the Administration's proposal would.

The Fighting Fraud to Protect Taxpayers Act of 2011

The Fighting Fraud to Protect Taxpayers Act of 2011 (S. 890), introduced by Senator Patrick Leahy on May 5, 2011, also modifies the CFAA. Language in the bill would enlarge the scope of the password trafficking offense by removing the requirement that the computer affect interstate commerce or be used by the United States.[44] This is very similar to the Administration's proposal.

[39] 18 U.S.C. § 1962(d).

[40] 18 U.S.C. § 1964.

[41] *See* S. 1151, 112th Cong. § 101 (2011).

[42] *See* S. 1151, 112th Cong. § 103 (2011).

[43] *See* S. 1151, 112th Cong. § 103 (2011); *compare* 18 U.S.C. § 1030(c).

[44] See S. 890, 112th Cong. §6 (2011); 18 U.S.C. § 1030(a)(6).

Unlike the bill, the Administration's proposal would additionally expand the scope of the provision by protecting means of access other than simply passwords.

Author Contact Information

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

Jonathan Miller
Legal Intern
jhmiller@crs.loc.gov, 7-6845