Proposed security researcher protection for the Computer Fraud and Abuse Act (CFAA)

06/01/21

Annotated with footnotes. Proposed language is in *italics*.

18 USC 1030 – Fraud and related activity in connection with computers

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action[1] against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).[2] Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

> *(1) Affirmative defense – It shall be an affirmative defense to a civil action under this subsection for conduct that involves subclause (c)(4)(A)(i)(I)[3] that the defendant acted solely for the purpose of good faith security research.*[4]

---

[1] (g): The CFAA provides for both civil and criminal liability. Under existing law, subsection (g) applies only to civil actions, not criminal prosecution. The proposed researcher defense, in italics, would be under (g), so the defense would only apply to civil actions.

[2] (g): Under existing law, to bring a civil action under subsection (g) for a CFAA violation, the violation must involve one of these five factors listed in 1030(c)(4)(A)(i):

- I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
- II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- III) physical injury to any person;
- IV) a threat to public health or safety;
- V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

[3] *(g)(1):* This applies the researcher protection to civil suits involving the first factor listed above: economic loss to one or more persons aggregating at least $5,000 over one year. A civil suit may still proceed if the violation involves any of the other four factors: potential modification or impairment of medical care, physical injury, threat to public safety, or damage affecting certain US government computers.

[4] *(g)(1):* The researcher protection would apply solely to good faith security research, but not if the researcher has other purposes, such as hacktivism, sale of vulnerabilities, stock shorts, malicious intent, etc. The phrase "solely for the purpose of good faith security research" is included in the Library of Congress' 2018 exemption for security research to Sec. 1201 of the Digital Millennium Copyright Act (DMCA). See 37 CFR 201.40(b)(11)(i).

(e) As used in this section –

(13) The term "good faith security research" means good faith testing or investigation to detect one or more security vulnerabilities in software, hardware, or firmware of a protected computer for the purpose of promoting the security or safety of the software, hardware, or firmware.[5]

(A) The person carrying out such activity shall

(i) carry out such activity in a manner reasonably designed to minimize and avoid unnecessary damage or loss to property or persons; [6]

(ii) take reasonable steps, with regard to any information obtained without authorization, to minimize the information the person obtains, retains, and discloses to only that information which the person reasonably believes is directly necessary to test, investigate, or mitigate a security vulnerability;[7]

(iii) take reasonable steps to disclose any security vulnerability derived from such activity to the owner of the protected computer or the Cybersecurity and Infrastructure Security Agency prior to disclosure to any other party;[8]

(iv) wait a reasonable amount of time before publicly disclosing any security vulnerability derived from such activity, taking into consideration the following:
(I) the severity of the vulnerability,
(II) the difficulty of mitigating the vulnerability,

---

[5] *(e)(13):* The 2018 exemption for security research to DMCA Sec. 1201 uses a similar language: "for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, [...] and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines[...]" See 37 CFR 201.40(b)(11)(ii).

[6] *(e)(13)(A)(i):* To be eligible for the defense, researchers would need to take reasonable steps to ensure they do not cause any harm while accessing or damaging computers without authorization. The phrase "reasonably designed" signifies that the researcher should take objectively reasonable steps to prevent harm, but also recognizes that the researcher may not be responsible for unreasonably improbable risks. This provision also draws from the phrase "carried out in an environment designed to avoid any harm to individuals or the public" in the 2018 security research exemption to DMCA Sec. 1201. See 37 CFR 201.40(b)(11)(ii).

[7] *(e)(13)(A)(ii):* Researchers would need to take care to avoid collecting or disclosing data in excess of what is needed for security research. For example, public disclosure of an entire database is not necessary to correct a security flaw in the means of access to the database. This applies only to information obtained without authorization under CFAA during the course of the research, and not other types of information.

[8] *(e)(13)(A)(iii):* An act of security research may not detect a vulnerability, and the researcher defense should apply even in the absence of a finding of a vulnerability. However, if a security vulnerability is detected or derived from the research, the researcher must endeavor to first disclose it to the computer owner or CISA. This applies only to vulnerabilities derived from research subject to the CFAA security research defense, not vulnerabilities derived from other research.

(III) the willingness and ability of the owner of the protected computer to mitigate the vulnerability; and
(IV) international standards and industry best practices;[9]

(v) not publicly disclose information obtained without authorization that is
(I) a trade secret as defined under 18 USC 1839(3), without the permission of the owner of the trade secret; or
(II) the personally identifiable information of another individual, without the permission of that individual;[10] *and*

(vi) not use a nonpublic security vulnerability derived from such activity for any primarily commercial purpose prior to disclosing the vulnerability to the owner of the protected computer or the Cybersecurity and Infrastructure Security Agency.[11]

(B) Nothing in subsection (e)(13) shall be construed to prohibit or require public disclosure of security vulnerabilities derived from good faith security research.

(C) For purposes of subsection (e)(13), it is not a public disclosure to disclose a vulnerability or other information derived from good faith security research to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.

(D) For purposes of subsection (e)(13), the term "security vulnerability" shall have the meaning given the term in 6 USC 1501(17).[12]

* * *

[9] *(e)(13)(A)(iv):* While this provision does not prohibit public disclosure, it requires the researcher to wait a reasonable amount of time before doing so. The provision includes factors to consider in determining what is reasonable. Similar language is included in the Vulnerability Disclosure Policy of the Dept. of Defense. See HackerOne, DoD Vulnerability Disclosure Policy, Nov. 21, 2016, https://hackerone.com/deptofdefense.

[10] *(e)(13)(A)(v):* This is to prevent public disclosures of particularly sensitive personal or business information. Private disclosure is not prohibited, but note that *(e)(13)* and *(A)(ii)* require that the researcher use this information for security and reasonably believe this information is necessary to strengthen security. Like *(A)(ii)*, this applies only to information obtained without authorization under CFAA.

[11] *(e)(13)(A)(vi):* This is to prevent use of the security research defense to gain a commercial advantage in cybersecurity products or services before the results of that research are disclosed. The goal is to avoid a scenario whereby a researcher finds a vulnerability and privately incorporates it into a commercial security product to gain a competitive edge, rather than disclose the vulnerability to strengthen security more broadly. Like *(A)(iii)*, this applies only to vulnerabilities derived from research subject to the CFAA security research defense.

[12] *(e)(13)(D):* As defined by the Cybersecurity Information Sharing Act of 2015, the term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.