9-48.000 - COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act ("CFAA"), codified at Title 18, United States Code, Section 1030, is an important law for prosecutors to address cyber-based crimes. As technology and criminal behavior continue to evolve, however, it also remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law.

To accomplish these goals, the Department has developed the following policy to guide attorneys for the government in the appropriate considerations for prosecutors contemplating charges under the CFAA.

A. *Consultation Requirements*

1. **Introduction**

   Cases under the CFAA are often complex, and analysis of whether a particular investigation or prosecution is consistent with the charging policy described below often requires a nuanced understanding of technology, the sensitivity of information involved, tools for lawful evidence gathering, national and international coordination issues, and victim concerns, among other factors. JM § 9-50.000 sets forth general requirements for cyber prosecutions, including coordination with and notification of the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division in certain cases.

2. **Investigative Consultation**

   As the best practice, the attorney for the government should consult with a Computer Hacking and Intellectual Property Coordinator ("CHIP") within the District in which the case would be brought at all important stages of an investigation, including the issuance of legal process to obtain electronic evidence. However, because electronic evidence is often subject to deletion after very short retention periods, the need to preserve or obtain evidence critical to the investigation may require taking preliminary investigative steps before undertaking the consultation above. In such cases, the consultations should take place as soon as possible.

3. **Charging Consultation**

   With respect to charging decisions, the attorney for the government shall consult with CCIPS to identify potential factual, legal, or policy issues, assist with deconfliction with similar cases in other Districts (to the extent the attorneys have not already completed such deconfliction pursuant to other Department policies and procedures), and review how the case relates to national priorities. Attorneys for the government are encouraged to have a District CHIP participate in this consultation. The consultation should be substantive in nature. It is meant to both assist the prosecutor and promote consistency in the Department in a quickly

evolving area of practice. The depth of the consultation and degree of information required to accomplish these goals will vary according to the facts, complexity, and sensitivity of a particular investigation or matter. These types of consultations are already a hallmark of the CHIP program, and the strong working relationships are a key reason for the program's collaborative successes.

4. **Consultation for Cases Involving National Security Issues**

For CFAA cases involving international terrorism or domestic terrorism, or affecting, involving, or relating to the national security, JM §§ 9-2.136, 9-2.137, 9-90.020, and/or 9-90.800 set forth additional NSD notification, consultation, and approval requirements, including those at the opening and investigative stages. In such cases, the attorney for the government can, if he or she chooses, satisfy the CCIPS and NSD charging consultation requirements with one contact. NSD or CCIPS will then be responsible for facilitating any additional charging consultations with the other component. If there is any question about whether a matter involves international terrorism, domestic terrorism, or otherwise affects, involves, or relates to the national security, the attorney for the government should consult with the National Security Cyber Specialist ("NSCS") within his or her District for further guidance.

5. Notification to the Office of the Deputy Attorney General

When an office has consulted with CCIPS and intends to charge a CFAA case in a manner contrary to a written recommendation invoking this paragraph, that office shall inform the Office of the Deputy Attorney General before charging. This policy does not affect the existing relevant procedures for appealing an NSD decision not to approve a CFAA case involving international terrorism or domestic terrorism, or that affects, involves, or relates to the national security. In no instance will an office charge a defendant with "exceeding authorized access" or "exceeds authorized access" contrary to a recommendation from CCIPS without approval from the Office of the Deputy Attorney General.

B. *Charging Policy for CFAA cases*.

1. Access "without authorization."

Section 1030 describes a number of offenses that occur when a defendant accesses a protected computer "without authorization." *See* 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(3), (a)(4), and (a)(5)(B)-(C). The Department will not charge defendants for accessing "without authorization" under these paragraphs unless when, at the time of the defendant's conduct, (1) the defendant was not authorized to access the protected computer under any circumstances by any person or entity with the authority to grant such authorization; (2) the defendant knew of the facts that made the defendant's access without authorization; and (3) prosecution would serve the Department's goals for CFAA enforcement, as described below in B.3.

2. Access "exceeding authorized access."

Three paragraphs of section 1030 describe offenses involving conduct that "exceeds authorized access," sometimes also phrased "exceeding authorized access." *See* 18 U.S.C. §§ 1030(a)(1), (a)(2), and (a)(4). The Department will not charge defendants with "exceeding authorized access" or "exceeds authorized access" under these paragraphs unless, at the time of the defendant's conduct, (1) a protected computer is divided into areas, such as files, folders, user accounts, or databases; (2) that division is established in a computational sense, that is, through computer code or configuration, rather than through contracts, terms of service agreements, or employee policies; (3) a defendant is authorized to access some areas, but unconditionally prohibited from accessing other areas of the computer; (4) the defendant accessed an area of the computer to which his authorized access did not extend; (5) the defendant knew of the facts that made his access unauthorized; and (6) prosecution would serve the Department's goals for CFAA enforcement, as described below in B.3.

3. Whether prosecution would serve the Department's goals for CFAA enforcement.

The Department's goals for CFAA enforcement are to promote privacy and cybersecurity by upholding the legal right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information systems.

Thus, in addition to the considerations set forth in JM § 9-27.230, which are incorporated herein by reference, an attorney for the Department of Justice should consider the following additional factors in determining whether a CFAA prosecution should be pursued because a substantial federal interest would be served by prosecution in a case in which the admissible evidence is expected to be sufficient to sustain a conviction:

1. The sensitivity of the affected computer system or the information transmitted by or stored on it and the likelihood and extent of harm associated with damage or unauthorized access to the computer system or related disclosure and use of information;
2. The degree to which damage or access to the computer system or the information transmitted by or stored on it raises concerns pertaining to national security, critical infrastructure, public health and safety, market integrity, international relations, or other considerations having a broad or significant impact on national or economic interests;
3. The extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm or a threat to national security;
4. The impact of the crime and prosecution on the victim or other third parties;
5. The deterrent value of an investigation or prosecution, including whether the need for deterrence is increased because the activity involves a new or expanding area of criminal activity, a recidivist defendant, use of a novel or sophisticated technique, or abuse of a position of trust or otherwise sensitive level of access, or because the conduct is particularly egregious or malicious;

6. The nature of the impact that the criminal conduct has on a particular District or community;

7. Whether any other jurisdiction is likely to prosecute the criminal conduct effectively, if the matter is declined for federal prosecution; and

8. The attorney for the government should decline prosecution if available evidence shows the defendant's conduct consisted of, and the defendant intended, good-faith security research. For purposes of this policy, the attorney for the government should apply the definition of "good-faith security research" recommended by the Register of Copyrights in *Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention,* at 258 (Oct. 2021). That is: "good faith security research" means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called "research," but is not in good faith. CCIPS can consult with prosecutors about specific applications of this factor.

C. *Comment.*

The Department will not bring "exceeds authorized access" cases based on the theory that a defendant's authorization to access a particular file, database, folder, or user account was conditioned by a contract, agreement, or policy, with the narrow exception of contracts, agreements, or policies that entirely prohibit defendants from accessing particular files, databases, folders, or user accounts on a computer in all circumstances. A CFAA prosecution may not be brought on the theory that a defendant exceeds authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or web service available to the general public—including public websites (such as social-media services) that allow for free or paid registration without human intervention. Also, a CFAA prosecution may not be brought on the theory that an employee has used a computer generally designated for his or her exclusive use in a way the employer's policy prohibits—for example, by checking sports scores or paying bills at work. However, an "exceeds authorized access" CFAA prosecution may be brought, for example, against a defendant who accesses a multi-user computer or web service, and is authorized to access only his own account on that computer or web service, but instead accesses someone else's account.

The Department also will not bring "exceeds authorized access" cases based on the theory that authorization to access a computer, or a particular area on a computer, was automatically withdrawn under the terms of a contract or other written document once the user did something, or some other particular condition was met. Thus, embellishing an online dating profile contrary to the terms of service of the dating website; creating fictional accounts on hiring, housing, or rental websites; or using a pseudonym on a social networking site that prohibits them, might all

violate a user's contract with the owner of the protected computer, but the Department will not take the position that a mere contractual violation caused the user's previous authorization to be automatically withdrawn and that the user was from that point onward acting in violation of the CFAA. However, when authorizers later expressly revoke authorization—for example, through unambiguous written cease and desist communications that defendants receive and understand—the Department will consider defendants from that point onward not to be authorized.

In either a "without authorization" case or an "exceeds authorized access" case, the attorney for the government must be prepared to prove that the defendant knowingly accessed a computer or area of a computer to which he was not allowed access in order to obtain or alter information stored there, and not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it. As part of proving that the defendant acted knowingly or intentionally, the attorney for the government must be prepared to prove that the defendant was aware of the facts that made the defendant's access unauthorized at the time of the defendant's conduct. Such an awareness could potentially be proven through various means, including the presence of technology intended (however unsuccessfully) to limit unauthorized access; written or oral communications sent to the defendant that unambiguously informed him that he is not authorized to access a protected computer or particular areas of it; or the defendant's own statements or behaviors reflecting knowledge that his actions were unauthorized. Experience has demonstrated that in the large majority of "exceeds authorized access" cases brought by the Department, the operator of the computer system made some technological effort to protect the information at issue, thereby signaling the importance or sensitivity of that information. It is not necessary that this technological effort erect an impenetrable "technological barrier" or that the technology succeed in its intended purpose of preventing access. To the contrary, when the CFAA is violated, the technology all too often "permits" the defendant's illegal access, often despite network defenders' unsuccessful technological attempts to prevent it.

The charging policy and principles set forth in this Justice Manual section, and internal office procedures adopted pursuant to this section, are intended solely for the guidance of attorneys for the government. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States.

[updated May 19, 2022]