# CRITICAL UPDATE NEEDED:

# WHY THE FEDERAL COMPUTER CRIME LAW IS WOEFULLY OUTDATED, AND HOW TO MODERNIZE IT

ANAND RAMASWAMY*

*Ransomware gangs drain billions from victims and put lives at risk by targeting hospitals and health care more than any other sector. Most of those groups operate from the countries of the former Soviet Union, well beyond the reach of U.S. law enforcement. However, the most significant ransomware attack on an American target was not against a hospital, but against the Colonial Pipeline, the gasoline pipeline supplying most of the U.S. East Coast in May 2021. A flurry of federal action followed the Colonial Pipeline incident, but oddly, Congress made no change to the single federal statute criminalizing computer fraud and abuse.*

*The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, predates the modern internet and lacks effective means to punish conspiracies or coordinated ransomware attack groups. Even if a Colonial Pipeline attacker had been convicted under the CFAA, the maximum punishment likely would not have exceeded ten years. If charged under the CFAA, a cybercriminal causing global disruption faces no more time in prison than a felon caught with a single bullet. That disparity in the potential degree of harm versus punishment is worthy of reformulation.*

*This article examines the origin of the Computer Fraud and Abuse Act, born from a question President Ronald Reagan posed after watching the movie WarGames, through its general stagnation as the internet, computers, and online criminal activity exploded in scope. After looking at why section 1030 is difficult to apply in criminal prosecutions, this article then analyzes other statutes criminalizing online enterprises. These examples have the potential to inform policymaking decisions. The article surveys the current*

* **Disclaimer:** The author is an Assistant United States Attorney. The views, analysis, and opinions set forth in this article are solely those of the author and do not represent the official position or endorsement of the Department of Justice or the U.S. Attorney's Office for the Middle District of North Carolina, or the United States Government.

*state of ransomware activity, including substitute charges used against actors, before concluding with a draft new subsection for the CFAA aimed at enterprise actors who continue to exact a toll on victims worldwide.*



## INTRODUCTION

In May 2021, Americans felt the shock of victimization when a cybercriminal gang half a world away held the East Coast's primary supplier of gasoline for ransom.[1] Ensuing disruptions of the fuel

1. *See* Regional Emergency Declaration Under 49 C.F.R. § 390.23, Fed Motor Carrier Safety Admin., No. 2021-002 (May 9, 2021), https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/2021-05/ESC-SSC-WSC - Regional Emergency Declaration 2021-002 - 05-09-2021.pdf [https://perma.cc/9VZ5-TASM]; *see*

supply prompted an emergency declaration by President Biden and a spike in gasoline prices.[2] Colonial Pipeline Company paid a ransom in excess of $4 million and resumed operations after one week, but the fallout from the crime was just beginning.[3] The incident marked a watershed event for government action on cyberattacks, prompting a series of significant measures undertaken in its wake.[4] Those actions included a temporary relaxation of some rules in order to expedite the supply chain of gasoline as well as cybersecurity directives aimed at critical infrastructure.[5] The government even fined the victim company, Colonial Pipeline, $986,400 for probable violations related to control room management.[6] However, one potential countermeasure was left untouched: updating the *only* federal law against computer fraud and abuse for use against modern criminal organizations like the group who attacked the Colonial Pipeline Company. That law, the Computer Fraud and Abuse Act, ("CFAA"), 18 U.S.C. § 1030, is woefully outdated. Standing alone, the CFAA would have allowed punishment of up to ten years for the Colonial Pipeline attackers, strongly disproportionate to the harm and disruption caused by the criminals. This article begins by outlining the birth and early development of the CFAA, highlighting its stunted growth and inability to meet the demands of modern computer fraud and abuse, especially ransomware. This article then analyzes other laws aimed at curtailing enterprise-level

*also* Remarks by President Biden on the National Economy, 2021 DAILY COMP. PRES. DOC. 5 (May 10, 2021, 13:44 EDT), https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/05/10/remarks-by-president-biden-on-the-economy/ [https://perma.cc/UJ95-KCAA] ("And over the weekend, at my direction, the Department of Transportation issued an emergency order to loosen restrictions on truck drivers in order to allow more fuel to be transported via tanker.").

2. Joseph Marks, *One Year Ago, Colonial Pipeline Changed the Cyber Landscape Forever*, WASH. POST (May 6, 2022), https://www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/ [https://perma.cc/AA5F-4U4L].

3. *Id.*

4. *Id.* ("It marked a seismic shift in which a cyberattack had real-world implications for tens of thousands of average Americans who spent hours in gas lines and fretted about price surges and being unable to fill their tanks. . . The government response was also unprecedented.").

5. *FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident*, THE WHITE HOUSE (May 11, 2021, 18:00 EDT), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/ [https://perma.cc/9SAP-LPU8].

6. Notice of Probable Violation Proposed Civil Penalty and Proposed Compliance Order, CPF 3-2022-026-NOPV, U.S. DEP'T OF TRANSP. (Pipeline and Hazardous Materials Admin. May 5, 2022), https://www.phmsa.dot.gov/news/phmsa-nopv-pcp-pco-to-colonial-pipeline-company [https://perma.cc/QY72-S2F9] [hereinafter Notice to Colonial Pipeline] (notice addressed to Colonial Pipeline, Co.).

criminal activity to glean useful features for an enterprise-based revision of the CFAA. This analysis covers the operation of modern malicious software (malware) and ransomware and the severe costs in money and human safety posed by ransomware. Finally, a proposed new subsection for the CFAA aimed at cybercriminal enterprises affecting computers is offered in the Appendix. This proposed new subsection draws from other enterprise laws examined herein to target the most culpable actors in the network with penalties proportionate to harm done, while including thresholds designed to exclude *de minimis* offenders.

## I. BACKGROUND

### *A. The Origin and Development of the U.S. Anti-Hacking Law*

Understanding the CFAA's shortcomings against modern malware gangs like the one behind the Colonial Pipeline attack requires understanding the environment in which the CFAA originated. After President Reagan watched *WarGames*, the 1983 movie about a hacker's access of a government computer which nearly triggered a global nuclear war, he asked cabinet officials and some members of Congress if such a scenario was possible. [7] When President Reagan was later told that the film's scenario was a possibility,[8] the push for a federal anti-hacking law soon saw results as part of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ("the 1984 Act").[9] When the 1984 Act was passed, only 87,073, or 8.2 percent of U.S. households had a computer.[10] Government regulation at that time essentially banned commercial internet use, [11] so few contemporaneous statistics on internet use existed. The U.S. Census Bureau only began tracking home internet use in 1997.[12]

---

7. FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 2 (2017).

8. *Id.* at 2; *See also* Seth Rosenblatt, *Where Did the CFAA Come From, and Where is it Going?*, THE PARALLAX VIEW (Mar. 16, 2016), https://www.the-parallax.com/where-cfaa-going-timeline-history/ [https://perma.cc/9NRJ-S72P].

9. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. XXI, §§ 2101-2103, 98 Stat. 2190.

10. U.S. CENSUS BUREAU, *Appendix Table A. Computer and Internet Use in the United States: 1984 to 2009* (spreadsheet 2010), https://www.census.gov/data/tables/time-series/demo/computer-internet/computer-use-1984-2009.html [https://perma.cc/8Q7C-S3QS].

11. *See* N.S.F. OFF. OF INSPECTOR GEN., *Acceptable Use Policy*, *in* REVIEW OF NSFNET 38, 39 (1993), https://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt [https://archive.ph/zIAc] (based on the National Science Foundation's original conclusion that commercial use of the internet would have a negative effect on its objectives).

12. U.S. CENSUS BUREAU, *supra* note 10.

The 1984 Act was passed to prevent the basic adverse scenario depicted in *WarGames*: the unauthorized access of computers protected by executive orders, computers used by financial institutions, and computers operated for or on behalf of the U.S. Government.[13] The 1984 Act contained a provision making a conspiracy punishable by not more than one-half of the penalty of the underlying proscribed offenses in section 1030 (which range from misdemeanors to life imprisonment).[14] This provision was removed in 1986.[15] The intent in removal was "that such conduct be governed by the general conspiracy offense in 18 U.S.C. 371,"[16] a statute prohibiting conspiracies against or to defraud the United States. That rationale was in keeping with Congress's desire to limit the CFAA to a narrowly defined federal interest, in an era where commercial internet use was still prohibited by regulation.[17] Congress broadened the range of computers subject to the CFAA's protection in 1994 by replacing the term "federal interest computer" with "computer used in interstate commerce or communication."[18] That change expanded the scope of the CFAA, as courts have interpreted this to mean that any internet-connected computer is a protected computer under the statute.[19]

### *B. Conspiracy Restored – Maybe*

The restoration of a conspiracy subsection to the CFAA in 2008 suffered from, and continues to suffer from, a lack of well-defined penalties in the restored subsection. The 2008 additional language to section 1030(b) appears here in italics: "Whoever *conspires to commit or* attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."[20] However, no contemporaneous revision of the penalty provisions in subsection (c) occurred. If the intent of Congress was to make conspiracies as punishable as the underlying offense in section 1030, that intent has not been recognized by the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice, which cautions federal prosecutors against

13. 18 U.S.C. § 1030(a) (1984).
14. *Id.* § 1030(b)(2).
15. S REP. NO. 99-432, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.
16. *Id.*
17. *See* N.S.F. OFF. OF INSPECTOR GEN., *supra* note 11.
18. S. REP. NO. 104-357, at 10 (1996).
19. United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (holding that computers of a non-profit organization were used in interstate commerce and communication, as they were connected to the internet).
20. 18 U.S.C. § 1030(b) (effective Sept. 25, 2008) (emphasis added); *see also* 154 CONG. REC. H8075-01 (2008).

relying on section 1030 conspiracy charges "due to the lack of clarity on penalties."[21] CCIPS acts as a *de facto* gatekeeper for any federal district charging under section 1030, requiring a pre-charge consultation before a district charges under the statute.[22] The result is an unused and thus essentially useless provision aimed at prosecuting conspiracies to hack computers, despite the statement in the 1996 legislative history of the CFAA that "Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime."[23] Simply put, the CFAA has *never* been updated to combat the malware/ransomware era Americans have endured for the past decade.

### *C. Rise of the Danger*

While the CFAA as the primary federal anti-hacking law remains static, organized criminal hacking has risen exponentially.[24] In the infancy of the computer age, the earliest malware might not have been considered malicious, as it did not truly stop a computer's operation but simply displayed messages to the user.[25] Monetization of computer disruption arose contemporaneously with CFAA's 1986 revision, and was first seen in software, which when duplicated without being licensed, disabled computers from booting and properly operating; instead, screens displayed a message with offers of remediation if the licensing fee was paid.[26] Because those developers provided their names and contact information, relying on victims' guilt to leave the incident unreported, it was not quite ransomware in the modern sense.[27] But the first true ransomware soon followed—the "AIDS

21. U.S. DEP'T OF JUST. COMPUT. CRIME AND INTELL. PROP. DIV., PROSECUTING COMPUTER CRIMES 55-56 (2015), https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ccmanual_0.pdf [https://perma.cc/8ZN6-3HT9].

22. *See* U.S. DEP'T OF JUST., JUSTICE MANUAL § 9-48.000 (2022), https://www.justice.gov/jm/jm-9-48000-computer-fraud [https://perma.cc/YZT2-83KU].

23. S. REP. NO. 104-357, *supra* note 18, at 5.

24. *See 2024 Cyber Security Statistic: The Ultimate List of Stats, Data, & Trends, Malware*, PURPLESEC (2024) (showing graph and statistics of malware infection growth rate as 12.4 million in 2009, and 812.67 million in 2018), https://purplesec.us/resources/cyber-security-statistics/-Malware [https://perma.cc/4P4T-79BV].

25. Val Saengphaibul, *A Brief History of the Evolution of Malware,* FORTINET (Mar. 15, 2022), https://www.fortinet.com/blog/threat-research/evolution-of-malware [https://perma.cc/NE2B-FHV7].

26. Saad Hasan, *The Making of the First Computer Virus — The Pakistani Brain*, TRTWORLD (Dec. 18, 2019), https://www.trtworld.com/world/article/12731383 [https://perma.cc/4G5V-MSKQ].

27. *Id.*

trojan," which encrypted victims' files and demanded a payment for decryption.[28] That scheme failed because its components were not yet fully developed: it spread by floppy discs sent through the mail, and payment was sought by check or money order sent to a post office box.[29] Such weak points of distribution and anonymous payment reception would soon be remedied by the rise of high-speed networking and cryptocurrency.

Except for some programs called 'worms' that expanded and clogged computer systems but made no extortionate demands to fix those systems,[30] the earliest malware described above often spread through what would now be seen as primitive means: insertion of media to a system, i.e., the floppy disc. This vector suited its era, as the internet was in its early stage of development. Three decades after the CFAA's passage, computers and high-speed internet reached nearly universal adoption in American households, from a starting point of zero—an astonishing level of growth with no commensurate substantive changes in the CFAA.

### *D. Evolution to Modern Ransomware*

Ransomware progressed in subsequent years and was the subject of academic theorizing,[31] but it was still hampered by the absence of a secure and untraceable means for criminals to receive ransom payments. In a 2012 scheme, bad actors posing as the FBI directed victims to pay supposed fines using prepaid money service cards.[32] But a few years earlier, in the wake of the 2008 global financial crisis, a blueprint for building a decentralized anonymous payment system appeared pseudonymously from "Satoshi Nakamoto,"[33] ostensibly as a means of taking control of money away from those who could subject it to inflation.[34] Dubbed "Bitcoin," the concept became operational the following year and

28. Kaveh Waddell, *The Computer Virus That Haunted Early AIDS Researchers*, ATLANTIC (May 10, 2016), https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/ [https://perma.cc/6RCX-ZPH4].

29. *Id.*; *see also* Saengphaibul, *supra* note 25.

30. *What Is the Morris Worm? History and Modern Impact?,* OKTA (Aug. 29, 2024), https://www.okta.com/identity-101/morris-worm/ [https://perma.cc/BJ73-YBZR].

31. A. Young and Moti Yung, *Cryptovirology: Extortion-Based Security Threats and Countermeasures,* IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 129–140 (1996).

32. FBI, *New Internet Scam: 'Ransomware' Locks Computers, Demands Payment* (Aug. 9, 2012), https://www.fbi.gov/news/stories/new-internet-scam [https://perma.cc/QJ9R-CRXH].

33. Satoshi Nakamoto, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/8JLL-25DH].

34. *Id.* at 4 ("Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.").

first became incorporated as a means of ransomware payment in 2013's CryptoLocker malware.[35] Ten years later, over 72 percent of businesses worldwide reported being affected by ransomware attacks in a trendline that has steadily risen.[36]

The consensus of observers is that malware/ransomware gangs largely reside in the nations of the former Soviet Union,[37] generally thwarting apprehension and extradition to the U.S. The criminal organizations themselves have undergone increasing diversification and specialization[38] in a criminal imitation of a business model. In a criminal version of the "gig economy," these organizations may not be hierarchical, but rather feature piecemeal work by affiliates in service to higher controlling levels.[39] While the Russia-Ukraine conflict has strained some relationships among these criminal organizations,[40] they continue because the illicit profits are astronomical. Cryptocurrency payments attributable to ransomware reached $765 million in 2020 and $766 million in 2021, although the amount fell to $457 million in 2022 as more victims refused to pay.[41] Government reports are even higher than the $766 million figure for 2021, tracking $1.2 billion in ransomware payments for that year.[42] These figures represent only amounts

35. Ryan W. Neal, *CryptoLocker Virus: New Malware Holds Computers for Ransom, Demands $300 Within 100 Hours and Threatens to Encrypt Hard Drive*, INT'L BUS. TIMES (Oct. 21, 2013, 15:23 EDT), https://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt [https://perma.cc/S887-GC52] (a contemporary account of first cryptographic malware / ransomware).

36. *Businesses Worldwide Affected by Ransomware 2018-2025*, STATISTA (Nov. 28, 2025), https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/ [https://perma.cc/6HZY-7CP4].

37. *See Statement before the H. Comm. on Fin. Services* (Apr. 27, 2023), https://www.fincen.gov/system/files/2023-04/HHRG-118-HFSC-DasH-20230427.pdf [https://perma.cc/9PXB-WY8F] (statement of Himamauli Das, Acting Director, FinCEN) ("Based on our analysis, Russia-related ransomware variants accounted for 69% of ransomware incident value, 75% of ransomware-related incidents, and 58% of unique ransomware variants reported for incidents in the review period. All of the top five highest grossing ransomware variants are connected to Russian cyber actors.").

38. *See, e.g.*, Kevin Townsend, *Access Brokers and Ransomware-as-a-Service Gangs Tighten Relationships,* SECURITYWEEK (June 2, 2022, at 10:45 AM ET), https://www.securityweek.com/access-brokers-and-ransomware-service-gangs-tighten-relationships/ [https://perma.cc/Q3PX-RLDA].

39. CHAINALYSIS, *The 2023 Crypto Crime Report* (2023), https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/ [https://perma.cc/6YFV-L4L5].

40. Joseph Marks, *11 Big Takeaways From the Conti Ransomware Leaks,* WASH. POST (Mar. 18, 2022), https://www.washingtonpost.com/politics/2022/03/18/11-big-takeaways-conti-ransomware-leaks/ [https://perma.cc/N75L-CJZR].

41. CHAINALYSIS, *supra* note 39, at 27.

42. *See* FINCEN, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JULY 2021 AND DECEMBER 2021 4, U.S. TREAS. (Nov. 1,

received by ransomware attackers, and not any associated costs of business disruption, remediation, lost profits, and additional insurance.[43] The true cost of ransomware likely defies calculation. This dire situation finds no parallel development in U.S. law to combat these threats.

### *E. Penalties Static While Harm Grew*

The CFAA's penalties for substantive offenses lack the teeth of similar federal statutes. The penalties found in the CFAA are no more than half those seen in comparable federal laws against mail fraud[44] and wire fraud,[45] subject to some exceptions. Both mail fraud and wire fraud generally have twenty-year statutory maximum sentences, but in the absence of a prior conviction or an intentional or reckless attempt to cause serious bodily injury or death, most offenses in the CFAA are capped at ten years.[46] If a ransomware actor faced a charge of extortion involving computers under section 1030(a)(7), the maximum sentence would be a mere five years absent a prior conviction under section 1030.[47]

These penalties are grossly disproportionate to offenses which cause harm that aggregates to billions of dollars,[48] so prosecutors routinely charge cybercriminal organization members with non-computer fraud crimes carrying longer potential sentences.[49] For example, cybercriminals are routinely charged with wire fraud, and while mail fraud and wire fraud are both predicate crimes upon

---

2022), https://www.fincen.gov/system/files/2022-11/Financial Trend Analysis_Ransomware FTA 2_508 FINAL.pdf [https://perma.cc/T7P9-XMLX].

43. U.S. Gov't Accountability Off., *Rising Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability*, GAO WATCHBLOG (July 19, 2022), https://www.gao.gov/blog/rising-cyberthreats-increase-cyber-insurance-premiums-while-reducing-availability [https://perma.cc/BME8-VJYF].

44. 18 U.S.C. § 1341.

45. 18 U.S.C. § 1343.

46. *Compare* 18 U.S.C. § 1343 (mail fraud and wire fraud having twenty-year maximum sentences), with U.S. DEP'T OF JUST. COMPUT. CRIME AND INTELL. PROP. DIV., *supra* note 21, at 3 tbl. 1 (most CFAA offenses having ten-year maximum sentences).

47. 18 U.S.C. § 1030(a)(7), (c)(3)(A).

48. *See* FINCEN, *supra* note 42, at 4.

49. *See, e.g.*, Indictment at 1, United States v. Evgeniy Bogachev, No. 2:14-cr-00127 (W.D. Pa. filed May 19, 2014) (charging conspiracy to defraud the U.S., fraud by computer, wire fraud, bank fraud, and money laundering); Arrest Warrant, United States v. Alla Witte, No. 1:21:mj-02236-AOR (N.D. Ohio filed Feb. 8, 2021) (charging conspiracy to defraud the U.S., conspiracy to commit wire and bank fraud, aggravated identity theft, wire fraud, bank fraud, and conspiracy to commit money laundering); Indictment at 1, United States v. Maksim Galochkin, No. 3:23-cr-92 (M.D. Tenn. filed June 12, 2023) (charging conspiracy to defraud the U.S., conspiracy to commit wire fraud, and wire fraud); Indictment at 1, United States v. Mikhail Tsarev, No. 1:23-cr-309 (N.D. Ohio filed June 15, 2023) [hereinafter Tsarev Indictment] (charging conspiracy to defraud the U.S. and wire fraud, money laundering, and a sentencing enhancement for a false registration of a domain name).

which prosecutions can be made under the Racketeer Influenced and Corrupt Organizations Act ("RICO")[50]—potentially holding one criminal actor accountable for the acts of an organization—a crime under the CFAA is not a RICO predicate crime. Nor is a crime under the CFAA a predicate crime under the money laundering statutes, 18 U.S.C. §§ 1956 and 1957. Merely restoring the penalty section for conspiracies in its original version is of no avail, as the penalties were fixed at no more than one half of the maximum for the intended offense. A model for retooling the computer fraud statute for use against modern cybercrime organizations may lie outside federal fraud statutes and within those statutes contemplating another aspect of criminal conduct: enterprise.

## II. ANALYSIS

As the single federal hacking law, the CFAA needs an enhanced penalty provision to address modern malware at the enterprise level, because the internal CFAA conspiracy subsection has indefinite penalty provisions and the general section 371 conspiracy statute's maximum penalty is only five years. Lessons can be gleaned from existing federal laws and sentencing guidelines aimed at addressing enterprise-level offenses, which use thresholds of activity as gatekeeping provisions for enhanced punishment. These federal statutes and guidelines are most notably seen in (1) the Racketeer Influenced and Corrupt Organization Act ("RICO");[51] (2) the Continuing Criminal Enterprise statute ("the "Kingpin Statute");[52] (3) the Continuing Financial Crimes Enterprise statute ("CFCE");[53] and (4) the Child Exploitation Enterprise statute ("CEE"). [54] Each is addressed below in a brief examination of those laws' impetus, thresholds, and punishments.

### *A. Other Enterprise Laws Examined: The RICO Act*

Congress sought "the eradication of organized crime in the United States"[55] by passing the RICO Act, stating that organized crime is" "a highly sophisticated, diversified, and widespread activity that annually drains billions of dollars from America's economy by unlawful conduct,"[56] a circumstance now seen with

50. 18 U.S.C. §§ 1961-1968.

51. Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 9, 84 Stat. 922, 941-48 (codified at 18 U.S.C. §§ 1961-68).

52. 21 U.S.C. § 848.

53. 18 U.S.C. § 225.

54. 18 U.S.C. § 2252A.

55. Pub. L. 91-452, § 1, Oct. 15, 1970, 84 Stat. 922.

56. *Id.*

modern ransomware. Rather than create a statute encompassing underlying crimes, the RICO Act referenced types of activity and over thirty existing federal and state crimes as constituting "racketeering" predicate offenses. Those included, *inter alia*, any federal or state felonious act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, obscenity, and narcotics.[57] Liability under the RICO Act requires a "pattern of racketeering activity," i.e., two or more acts of racketeering activity in a ten-year period (excluding any prison sentence).[58] "The elements of a substantive RICO offense consist of (1) the conduct (2) of an enterprise (3) through a pattern of racketeering activity."[59] A RICO "'enterprise' includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity."[60] The broad reach of the RICO Act extends to any person employed by or associated with any enterprise engaged in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt,[61] leading courts to conclude that "the RICO net is woven tightly to trap even the smallest fish, those peripherally involved with the enterprise."[62] Individuals, corporations, and other entities may constitute an association-in-fact under RICO's definition of what constitutes an enterprise.[63]If the RICO Act has potential to be a guide for a revised CFAA, some qualities of RICO bear further examination. First, Congress directed that the RICO Act "shall be liberally construed to effectuate its remedial purposes."[64] In interpreting the RICO Act, courts have stated, "We would deny society the protection intended by Congress were we to hold that the Act does not reach those enterprises nefarious enough to diversify their criminal activity."[65] RICO defendants need not have committed underlying offenses so long as they had a role in the conduct. RICO contains a conspiracy section with elements differing from its substantive act provisions, such that courts have held "a substantive RICO violation and a RICO conspiracy are not the same offense for double jeopardy

57. 18 U.S.C. § 1961(1).

58. 18 U.S.C. § 1961(5) (stating that at least one such act of racketeering occurred after the date the RICO Act became law: Oct. 15, 1970).

59. United States v. Velazquez-Fontanez, 6 F.4th 205, 212 (1st Cir. 2021) (internal citations and quotation marks omitted).

60. 18 U.S.C. § 1961(4).

61. 18 U.S.C. § 1962(c).

62. United States v. Elliott, 571 F.2d 880, 903 (5th Cir. 1978).

63. United States v. Perholtz, 842 F.2d 343, 353 (D.C. Cir.1988) (collecting cases).

64. 18 U.S.C. §§ 1961-68.

65. *See Elliott*, 571 F.2d at 899.

purposes, and accordingly, can be punished separately."[66] Violators of RICO's section 1962 face imprisonment for up to twenty years or life, if the predicate crime is punishable by imprisonment for life.[67] The RICO Act thus relies on any two or more existing predicate offenses if committed in a pattern (i.e., within ten years excluding time in prison) in an enterprise (association of persons), permitting punishment of up to twenty years (or life, if the underlying act is so punishable).

### *B. The Drug Kingpin Law*

In the same year the RICO Act was passed, Congress also passed a law aimed at enterprise-level narcotics operations: the Continuing Criminal Enterprise Statute ("CCE"), or "Kingpin Statute," codified at 21 U.S.C. § 848.[68] While the RICO Act imposes a twenty-year maximum imprisonment term (for predicate offenses punishable for less than a life sentence), convictions under the CCE Statute carry a twenty year *minimum* sentence, and a maximum of life imprisonment[69] for "super-kingpin"[70] offenders. Under this law, a continuing criminal enterprise occurs when a violator commits a felony drug offense under 21 U.S.C. Chapter 13, which is part of a continuing series of such violations undertaken in concert with five or more other persons, and the violator is an organizer, supervisor, or in any other position of management, thus obtaining substantial income or resources.[71] The CCE Statutes' mandatory life sentence provision sets even higher thresholds, mainly seen in drug quantity and criminal proceeds.[72] Unlike the RICO Act's broad reach, the CCE Statute's focus on leaders brings higher penalties, but recognizes that such leaders may not personally commit the acts underlying the statute: "Requiring personal commission of the predicate offenses would essentially knock out the sentencing enhancements that § 848 provides for kingpins, who delegate the dirty work."[73]

66. United States v. Marino, 277 F.3d 11, 39 (1st Cir. 2002).

67. 18 U.S.C. § 1963(a).

68. *See, e.g.*, United States v. Webster, 639 F.2d 174, 180 (4th Cir. 1981) ("21 U.S.C. § 848 [is] a provision which is sometimes called 'the kingpin statute' because it is designed to apply to ringleaders of large-scale illegal narcotics operations.").

69. 21 U.S.C. § 848(a).

70. Chapman v. United States, 500 U.S. 453, 467 (1991).

71. 21 U.S.C. § 848(c).

72. 21 U.S.C. § 848(b) (requiring that the violator be a principal administrator, organizer, or leader of the enterprise engaged in violations otherwise punishable by five to forty years in § 841(b)(1)(B) of this title, with the enterprise receiving $10 million or more in gross receipts within a twelve-month period).

73. United States v. Hoover, 246 F.3d 1054, 1058 (7th Cir. 2001).

### *C. The Financial Crimes Kingpin Law*

The Savings and Loan (S&L) crisis of the 1980s prompted the Continuing Financial Crimes Enterprise (CFCE) Statute, 18 U.S.C. § 225, which notably also used the term "kingpin"[74] to describe violators meriting enhanced criminal punishment of up to life in prison.[75] The thresholds for prosecution set in the CFCE statute are that the actor organizes, manages, or supervises a continuing financial crimes enterprise which receives $5 million or more in gross receipts during any twenty-four month period.[76] The law defines a "continuing financial crimes enterprise" as a series of violations of enumerated federal laws[77] affecting a financial institution, committed by at least four persons acting in concert.[78]

### *D. A Non-Monetary Example: Child Exploitation Enterprise*

The final example of enterprise in federal criminal law appears in child exploitation enterprises under 18 U.S.C. § 2252A(g). This is a subsection of the main federal statute criminalizing child pornography. Congress recognized that child pornography offenses inflict physiological, psychological, and emotional harm, as well as being a source of illicit profit. When child pornography offenses are committed by a criminal enterprise, offenders are subject to very harsh penalties that account for harm exceeding financial gain or loss.[79] Those penalties mandate a sentence of not less than twenty years, and may be as great as life imprisonment.[80]

---

74. The bill's title was the Financial Crime Kingpin Statute, which was enacted as part of the Crime Control Act of 1990. *See* Pub. L. No. 101-647, § 2510, 104 Stat. 4789, 4861 (codified as amended at 18 U.S.C. § 225); *see also* 136 CONG. REC. 16911 (1990) (statement of Sen. Biden) ("[W]e put a provision in this bill that we drafted, and it is called the kingpin provision.").

75. The bank fraud statute has a maximum sentence of thirty years. *See* 18 U.S.C. § 1344.

76. 18 U.S.C. § 225(a).

77. 18 U.S.C. § 225(b). The enumerated offenses are 18 U.S.C. §§ 215 (receipt of commissions or gifts for procuring loans), 656 (theft, embezzlement, or misapplication by bank officer or employee), 657 (fraud and false statements in lending, credit and insurance institutions), 1005 (fraud and false statements in bank entries, reports and transactions), 1006 (fraud and false statements in federal credit institution entries, reports and transactions), 1007 (fraud and false statements in Federal Deposit Insurance Corporation transactions), 1014 (fraud and false statements in loan and credit applications generally; renewals and discounts; crop insurance), 1032 (fraud and false statements in concealment of assets from conservator, receiver, or liquidating agent), 1344 (bank fraud), 1341 (mail fraud), and 1343 (wire fraud).

78. 18 U.S.C. § 225(b).

79. 18 U.S.C. § 2252A(g)(2) (enterprise offenses defined as committed as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and when committed in concert with three or more other persons).

80. 18 U.S.C. § 2252A(g)(1).

### *E. Comparing the Enterprise Laws*

Before considering what a computer fraud enterprise law might look like, a summary of the statutes examined above may be helpful. This table comparing enterprise crime statutes shows the common elements as well as the differences:

TABLE 1. Common and Distinct Elements of Enterprise Crime Statutes

| Statute | Leadership Role Required? | Action |
|---|---|---|
| RICO | No | Pattern of racketeering (two acts in ten yrs.) |
| CCE | Yes | Felony drug offense within a continuing series of violations |
| CFCE | Yes | Continuing series of enumerated financial crime violations within 24 months |
| Child Exploitation Enterprise | No | Three or more separate incidents involving more than one victim |

| Monetary Threshold | No. of Accomplices | Penalty (years) |
|---|---|---|
| None | | Up to 20 |
| Substantial income or resources | ≤ 5 | 20 to life* |
| Gross proceeds of $5 million or more | ≤ 4 | Any term up to life |
| N/A | ≤ 3 | 20 to life* |

* Higher penalties if the underlying offense is punishable by life imprisonment

The RICO Act should be examined further in the context of a computer fraud enterprise law, as it does not require a leadership role and does not have a threshold in the number of accomplices. Rather, RICO relies on a criminal actor's role within an "enterprise":

> An association-in-fact enterprise is simply a continuing unit that functions with a common purpose. Such a group need not have a hierarchical structure or a "chain of command"; decisions may be made on an ad hoc basis and by any number of methods—by majority vote, consensus, a show of strength, etc. Members of the group need not have fixed roles; different members may perform different roles at different times. The group need not have a name, regular meetings, dues, established rules and regulations, disciplinary procedures, or induction or initiation ceremonies. While the group must function as a continuing unit and remain in existence long enough to pursue a course of conduct, nothing in RICO exempts an enterprise whose associates engage in spurts of activity punctuated by periods of quiescence.[81]

That use of the term "enterprise" is very fitting for modern malware and ransomware gangs, and borrowing the same term could fortify any revision of the CFAA as the term could potentially allow well-developed RICO Act caselaw to be used by reference.

### *F. Application of Enterprise Law Principles to the Known State of Modern Computer Fraud Enterprises*

Defining "enterprise" within a new subsection of the CFAA should look to the benefits and drawbacks of each enterprise-type crime cited above to glean what is useful for addressing actions of malware and ransomware groups. That task requires some discussion of how those groups operate, "mirror[ing] the SaaS [Software as a Service] model in which the providers offer subscription-based services and software."[82] One example is LockBit, the most prolific ransomware group of recent years,[83] where the creators made a user-friendly product for affiliates willing to pay for the service.[84] In 2022, LockBit accounted for 16 percent of ransomware attacks on state, local, tribal, and territorial

81. Boyle v. United States, 556 U.S. 938, 948 (2009).

82. *RaaS vs SaaS*, HALCYON, https://www.halcyon.ai/raas-vs-saas [https://perma.cc/JLC7-FTV2]; *see* Chrystal R. China, *What is software as a service (SaaS)?*, IBM, https://www.ibm.com/topics/saas [https://perma.cc/U8LS-2V29].

83. *Power Rankings: Ransomware Malicious Quartile Q4-2023*, HALCYON (Jan. 1, 2024), https://www.halcyon.ai/raas-mq/q4-2023 [https://perma.cc/276A-QQGC] ("LockBit is by far the most prolific ransomware operation to date. . .").

84. *LockBit Ransomware: Inside the World's Most Active Ransomware Group,* FLASHPOINT: THREAT INTEL BLOG (July 20, 2023), https://flashpoint.io/blog/lockbit/ [https://perma.cc/K8GC-8PU4] ("The group continues to innovate both their methods of operation and their technical capabilities, and maintains its offering of an easy-to-use, effective malware that allows other threat actors to profit.").

(SLTT) governments in the U.S., raking in $91 million from American victims from the time the group was first observed in January 2020 until mid-2023.[85] According to a recent indictment:

The LockBit conspiracy operates through the "ransomware-as-a-service" model, or 'RaaS.' The RaaS model involves two related groups of ransomware perpetrators: developers and affiliates. The developers design the ransomware code itself—much as a software company would—and maintain the infrastructure, such as servers, on which LockBit operates. The developers then recruit and market their ransomware product to affiliates, who actually deploy the ransomware product designed by the developers.[86]

Because the LockBit developers have essentially used a franchise model, methods of actual attack and extortion are not uniform because they are carried out by franchisees or affiliates. LockBit ransomware attacks vary significantly "due to the large number of unconnected affiliates in the operation."[87] Because the affiliate model involves payment for ransomware as a service and partial distribution of the ransom back to the developer, a computer fraud and abuse enterprise law should thus have some nexus related to proceeds. This is preferable to a nexus related to a leadership role, where affiliates are unconnected from each other. One indictment of the Trickbot malware/ransomware group shows the challenges of treating virtual associations as enterprises for charging purposes. The group name can change frequently, and individuals involved may have never physically met.[88] The Trickbot Group developed from a prior malware group—Dyre—following a Russian police disruption of Dyre in 2014.[89] The indictment identified four higher-level managers and several mid-level managers working in various specialty areas including payroll, reporting, and coordination of operations.[90] The group placed job postings seeking computer programmers on Russian and Belarussian job websites. At least one applicant realized that the tasks and tests given to the applicants required illegal actions.[91] Defendants and co-conspirators, who appeared to work together only online, were identified by names—where revealed—and online

85. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (CISA), *Understanding Ransomware Threat Actors: LockBit*, (June 14, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a [https://perma.cc/PSP4-28VQ] [hereinafter *CISA LockBit*].

86. Indictment at 4–5, United States v. Sungatov, No. 24-80(SDW) (D.N.J. Feb. 5, 2024) [hereinafter Sungatov Indictment].

87. *See CISA LockBit*, *supra* note 85, at 2.

88. *See* Tsarev Indictment, *supra* note 49.

89. *Id.* at 9.

90. *Id.* at 25.

91. *Id.* at 26–32.

monikers. The criminal activity was also done online only, with criminal proceeds received through unauthorized wire transfers and online ransomware payments in virtual currency.[92] A revision to the CFAA should look to conduct within the enterprise, with recognition that these enterprises are not legal entities, and that enterprise names frequently change. For purposes of showing affiliation, the enterprise can be established by the flow of funds, online chat conversations, and use of malware and ransomware known to be obtained by payment to developers.

The criminal enterprise described in the Trickbot Group indictment comports well with the Supreme Court's description of an association-in-fact in *Boyle,* a case involving a burglary group prosecuted under the RICO Act.[93] In *Boyle*, a leaderless non-hierarchical group consisting of a core group and others recruited on occasion met *ad hoc* to conduct nighttime thefts from bank deposit boxes.[94] Similarly, the Trickbot Group had a core of managers acting with others in diverse roles, functioning as a unit long enough to engage in a criminal course of conduct. The indictment describes the association and specialized roles in detail:

> To perpetrate their criminal schemes, Defendants used a network of associates who provided specialized services and technical abilities in furtherance of the criminal scheme. The specialized skills and services included soliciting and recruiting malware developers; purchasing and managing servers from which to test, deploy, and operate the Trickbot malware; encrypting the malware to avoid detection by anti-virus software; engaging in spamming, phishing and spear-phishing campaigns against potential victims; and coordinating the receipt and laundering of funds from the victims to Defendants and others.[95]

Compare this approach to jointly undertaken criminal activity defined under the CEE and CFCE statutes, each of which requires that the defendant be a manager, supervisor, or leader.[96] Those statutes are aimed at "kingpins," while RICO functions as a means to prosecute members of a criminal unit. The latter approach is preferable where arrest and prosecution of *any* defendant in a

92. *Id.* at 20–21.
93. Boyle v. United States, 556 U.S. 938 (2009).
94. *Id.*
95. *Id.* at 10.
96. *See* 18 U.S.C. § 225(a)(1); *see also* 21 U.S.C. § 848(b)(1)(A).

major malware case would be a challenge. Otherwise, the approach would invite the defense to deny a managerial role.[97]

Consider the complex operation of what was once described as "the world's most dangerous malware."[98] Dubbed "Emotet," its dangerousness stemmed from its ability to be a delivery system for hire to other criminal organizations. Emotet used an extensive network of compromised computers (botnet) to spread itself through campaigns of spam emails with attachments which, once opened, activated a series of steps to infect a victim's computer.[99] Emotet could perform a number of nefarious activities, including stealing credentials, harvesting email addresses, distributing spam, and delivering payloads of other criminal organizations' malware—such as the Trickbot Group's ransomware.[100] Emotet is an example of Malware-as-a-Service (MaaS), designed to evade detection—including from anti-virus programs.[101] In 2014, Emotet evolved from a banking trojan to a highly-sophisticated 'dropper' (program that delivers malware to a system). Emotet was designed to detect if it was operating on a virtual machine (software-based operating environment used, among various purposes, to examine malware operation), a feature which thwarted its analysis.[102] At its peak, Emotet was linked to 70 percent of malware worldwide,[103] with an

97. *See Transnational Organized Crime Rewards Program: Evgeniy Mikhailovich Bogachev,* U.S. DEP'T OF STATE (Apr. 9, 2017), https://www.state.gov/transnational-organized-crime-rewards-program/evgeniy-mikhailovich-bogachev [https://perma.cc/4ZGZ-YXNA] (an example of the difficulty in apprehending cybercriminals is seen in the as-yet-uncollected $3 million reward offered since 2017 for a defendant outside the United States).

98. Press Release, EUROPOL, *World's most dangerous malware EMOTET disrupted through global action* (Jan. 27, 2021), https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action [https://perma.cc/L3DN-UEXG].

99. *Id.*

100. Danny Palmer, *Emotet, once the world's most dangerous malware, is back*, ZDNET (Nov. 16, 2021, 4:33 AM PT), https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/ [https://perma.cc/3PX4-MA8H]; *see also* Aaron Hambleton, *Emotet Malware 2023 Resurgence* (Mar. 23, 2023), CYBER MAG., https://cybermagazine.com/articles/emotet-malware-2023-resurgence [https://perma.cc/3ZJG-XVCD].

101. *Emotet Malware Over the Years: The History of an Infamous Cyber-Threat,* HEIMDAL (July 5, 2022), https://heimdalsecurity.com/blog/emotet-malware-history/ [https://perma.cc/H76K-3R54].

102. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (CISA), Alert: *Emotet Malware*, TA18-201A (Jan. 23, 2020), https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware [https://perma.cc/EW5C-5TGD] [hereinafter CISA Alert].

103. Alexander Martin, *Emotet: Police raids take down botnet that hacked 'millions of computers worldwide,'* SKY NEWS (Jan. 27, 2021, 16:31 GMT), https://news.sky.com/story/emotet-police-raids-take-down-botnet-that-hacked-millions-of-computers-worldwide-12200460 [https://perma.cc/Z98W-AMWT].

average remediation cost of $1 million for SLTT governments.[104] The sheer scale and complexity of a criminal operation like Emotet presents a challenge in charging any single actor under CFAA due to the diversity of roles; the CFAA does not lend itself to charging groups due to the sentencing gap in its conspiracy subsection. But a RICO Act-styled 'enterprise' addition to the CFAA could capture even the jointly-undertaken activity of two criminal organizations (e.g., Emotet and Trickbot), as a partnership or an association in fact.

### *G. A Crime Refined: The Cycles of Extortion*

The CFAA criminalizes extortionate demands with the punishment limited to five years[105] of imprisonment. However, modern ransomware groups have been using repeated phases of extortion to more fully monetize stages in the ransomware cycle.[106] The first phase is extortion by encryption: the tactic Crypto Locker's creators perfected in 2013.[107] By 2020, criminals added a second phase—double extortion—threatening to release exfiltrated sensitive data unless extortionate demands were met.[108] Triple extortion soon followed with distributed denial of service (DDoS) attacks if victims broke off negotiations with ransomware groups.[109] In quadruple extortion, criminals make demands of individuals involved in data breaches. For example, in 2020, a ransomware gang emailed Finnish psychiatric patients and threatened to release their patient records unless they paid about $200.[110] But paying ransom may not restore a victim to a pre-ransomware state. A 2024 survey of 1,008 IT cybersecurity professionals in companies victimized by ransomware revealed that 84 percent of companies paid the ransom, but less than half had

104. *See* CISA Alert, *supra* note 102.

105. 18 U.S.C. §§ 1030(a)(7), (c)(3)(A).

106. Janus Agcaoili et al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, TREND MICRO (June 15, 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti [https://perma.cc/HMB9-NXJW].

107. Neal, *supra* note 35.

108. Agcaoili et al., *supra* note 106.

109. *Id.*; *see also* Lucian Constantin, *REvil ransomware explained: A widespread extortion operation*, CSO (Nov. 12, 2021), https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html [https://perma.cc/8T62-9T8P].

110. *'Shocking' hack of psychotherapy records in Finland affects thousands*, GUARDIAN (Oct. 26, 2020, 12:18 EDT), https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland [https://perma.cc/HKA4-FS2G].

their data restored without corruption.[111] Paying ransom appears to encourage subsequent ransomware incidents, given 78 percent of those surveyed reported they were victimized again after paying ransom and 63 percent stating the ransom was *higher* in the subsequent attack.[112] The attached report states that artificial intelligence will enable ransomware groups to further refine their tactics by using AI to translate personalized social engineering as a means of gaining access and localizing attacks.[113] A computer hacking enterprise law could help modernize the CFAA to meet this kind of evolution of tactics.

### *H. Why Not RICO?*

A 2018 Department of Justice report suggested "[a]dding the CFAA as a predicate offense for RICO purposes could increase our ability to fight cybercrime and take down criminal organizations engaged in such activities."[114] The RICO Act arguably has the largest scope of any of the criminal enterprise statutes examined herein, broadened in part by a congressional mandate that RICO be liberally construed.[115] However, the RICO Act also contains the lowest sentencing range, capped at twenty years (except when the underlying offense is punishable by life).[116] Making the CFAA a predicate offense of the RICO Act may look like an easy solution to the problem of using the CFAA for jointly-undertaken cybercriminal activity, but it may expose the smallest fish caught in the RICO-net to a punishment disproportionate to the criminal act. A cautionary example of using the RICO Act in a cybercrime context is demonstrated by the 2013 conviction of a member of an illicit credit card forum who was just eighteen years old upon his arrest.[117] He was alleged in a RICO prosecution to have jointly possessed twenty-six blank cards based on access device fraud[118]

111. CYBEREASON, RANSOMWARE: THE TRUE COST TO BUSINESS 2024, at 7, https://www.cybereason.com/hubfs/dam/collateral/ebooks/Ransomware-True-Cost-2024-eBook.pdf [https://perma.cc/JA6L-MGH5].

112. *Id.*

113. *Id.* at 2.

114. U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE 122 (2018), https://www.justice.gov/archives/ag/page/file/1076696/download [https://perma.cc/EKU2-S6AB].

115. 18 U.S.C. §§ 1961-68.

116. 18 U.S.C. § 1963(a).

117. Danika Worthington, *Pheonix man gets 20 years for credit card, ID scheme*, AZ CENTRAL (May 15, 2014, 16:14 MT), https://www.azcentral.com/story/news/local/phoenix/2014/05/15/phoenix-man-gets-years-prison-credit-card-scheme-abrk/9146825/ [https://perma.cc/FDL8-9V7L].

118. *See* Indictment at 39, United States v. Defendant, 2012 U.S. Dist. LEXIS 53576, No. 2:12-cr-00004-APG-GWF (D. Nev. filed Jan. 10, 2012) [hereinafter Defendant Indictment]; *see also* 18 U.S.C. § 1029.

and was one of about 5,500 people associated with an illegal Russian-based carding forum—39 of whom were included in the indictment.[119] The eighteen-year-old received a twenty-year sentence and was ordered to pay $20 million in restitution for violations of 18 U.S.C. § 1962.[120] Compare that punishment to the punishment of a programmer who helped develop and deploy ransomware in the Trickbot Group: despite arguably having tremendous impact on victims worldwide,[121] the programmer received a sentence of only thirty-two months.[122] This disparity highlights—if nothing else—the significant role of the charges and plea agreements in hacking cases, as prosecutors in the latter case accepted a plea to a § 371 conspiracy, punishable at most by sixty months in prison.[123] Rather than being incorporated into the RICO Act or being a new, stand-alone statute, a law aimed at tackling organized criminal activity related to computers arguably belongs within the sole federal statute covering computer crimes: the CFAA. This approach comports with the legislative history of the CFAA, reflecting a desire to modernize section 1030 in order to provide law enforcement with the necessary tools to fight cybercrime.[124] Some elements of the RICO Act would be beneficial to a revamp of the CFAA. The addition of a computer fraud enterprise to section 1030 would benefit from borrowing the definition of 'enterprise' used in the RICO Act, as it may provide a well-established foundation in case law rather than being novel and subject to new interpretation. An identical definition of 'enterprise' would thus serve as an indicator to the contours of a new law on cybercrime enterprises. A threshold in the number of accomplices (as seen in CCE and CFCE) is less desirable, because identities may be difficult to ascertain for actors using online monikers in forums located outside the United States. The U.S. government would likely have to prove each moniker was that of an individual person to meet such a threshold, and as the Lockbit and Trickbot Group indictments show, actors have multiple online aliases.[125] As with

119. Worthington, *supra* note 117; *see also* Defendant Indictment, *supra* note 118, at 39–41.

120. *See* Worthington, *supra* note 117.

121. Tsarev Indictment, *supra* note 49, ¶ 178.

122. *Trickbot member pleads guilty in Cleveland, becomes U.S.' first conviction in probe into notorious Russian-based cyber gang*, CLEVELAND.COM (June 28, 2023, 14:42 EDT), https://www.cleveland.com/court-justice/2023/06/trickbot-member-pleads-guilty-in-cleveland-becomes-us-first-conviction-in-probe-into-notorious-russian-based-cyber-gang.html [https://perma.cc/9JTL-NJWJ].

123. *Id.* (what is not known is whether this defendant received the benefit of a reduction under USSG §5K1.1, Substantial Assistance to Authorities).

124. S. REP. NO. 104-357, *supra* note 18, at 3.

125. Tsarev Indictment, *supra* note 49, at 9; *see also* Sungatov Indictment, *supra* note 86, at 14–15.

the CCE and CFCE statutes, a monetary threshold may be well-placed in a computer fraud enterprise law to ensure it is used against violators on a scale worthy of enhanced punishment.[126] Such a monetary threshold could be proven by criminal proceeds, the costs of remediation borne by victims, and the demands in ransomware cases.

### *I. Addressing Opposition and Counterarguments to the Proposed Change in the CFAA*

Some may balk at beefing up penalties and the scope of liability of the CFAA, which has been widely criticized for vagueness in defining essential terms, its current potential for severe sentences, and its reliance on thin predication such as violations of a website's terms of service.[127] While some of those criticisms retain validity, many have ceased in relevance in light of courts' narrowing interpretations of the CFAA and some revisions of the statute. Nonetheless, past criticism of the CFAA would likely pose a challenge for adding an enterprise subsection with strong penalties, even if those are proportionate to the harm done. The criticisms are addressed below.

Subsections of the CFAA frequently use "accessing a computer without authorization or exceeding authorized access" as a basis of committing criminal acts, but the statute does not include sufficiently clear definitions of what those terms mean in practice.[128] Courts have since clarified those terms to a large degree, but the law pertains to "computers," a wide-ranging and growing swath of subtopics presenting ever-shifting challenges of application unforeseen when section 1030 was first enacted, including commercial use of the internet and websites' terms of service. For example, in a tragic incident in Missouri, prosecutors alleged the creation of a false online persona on a social media website as an act of "accessing a computer without authorization or

126. 18 U.S.C. § 225; *see also* Federal Criminal Case Processing Statistics Data Tool, BUREAU OF JUST. STAT., https://fccps.bjs.ojp.gov/home.html?dashboard=FJSP https://perma.cc/929Z-RXP2 (select "Home" on menu; click "United States Code Statistics" under "By Title and Section;" then select the "United States Code Group" drop-down menu and select "18—Crimes and Criminal Procedure;" then select the "United States Code citation" dropdown menu and deselect "all" and select "18:225") (chart depicting number of persons in cases filed under 18 U.S.C. § 225) [hereinafter Statistics Data Tool].

127. *See, e.g.*, Kelsey T. Patterson, *Narrowing it Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 491 (2013).

128. 18 U.S.C. § 1030(a)(1).

exceeding authorized access."[129] In 2006, a woman created a false online persona of a teen boy to romantically befriend and then reject her daughter's thirteen-year-old classmate, who then committed suicide.[130] Charged with felonies under the CFAA, the defendant was convicted on a single, lesser-included misdemeanor.[131] On appeal, the court noted that the terms "access[ing] a computer" and "without authorization" were undefined and subject to controversial interpretation. The court rejected predication of section 1030 on a terms-of-service violation based on the defendant's void-for-vagueness challenge.[132] In so holding, the court stated:

> If any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[133]

The Ninth Circuit subsequently held that the CFAA's "exceeding authorized access prong" is not met by someone violating a company's computer use policy.[134] Most recently, the Supreme Court reached the same conclusion in the context of a computer-use policy violation as a predicate for a section 1030 prosecution, recognizing that the alternative would "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook."[135] More technical means of exceeding authorized access, such as the use of proxy scanners to identify vulnerable servers and surreptitiously set up unauthorized operations, have been found to violate section 1030.[136] Despite clarification of essential terms within the CFAA by courts, some still fault the statute for vagueness, and this will likely cause resistance to an expansion of penalties.[137] In fact, stiffer criminal

129. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).
130. *Id.*
131. *Id.*
132. *Id.* at 458.
133. *Id.* at 467 (citing City of Chicago v. Morales, 527 U.S. 41 (1999)).
134. United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc).
135. Van Buren v. United States, 592 U.S. 374, 393 (2021).
136. United States v. Thompson, No. CR19-159RSL, 2022 WL 834026, at *2, *8 (W.D. Wash. Mar. 21, 2022).
137. *See, e.g.*, Orin S. Kerr, *Privacy, Property, and Crime in the Virtual Frontier: Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562.

penalties under the CFAA may be an uphill fight as some advocate for lesser penalties,[138] including for actual forms of cyberattacks if they constitute political protests and cause minimal harm.[139] The CFAA faces criticism for its potentially severe sentences, an allegation possibly based on common public misunderstandings of federal sentencing. As noted in an article advocating for a new Sentencing Guidelines provision specific to the CFAA, "[m]edia coverage of CFAA prosecutions routinely emphasizes statutory maximum sentences instead of Federal Sentencing Guidelines recommendations, fostering wildly unrealistic perceptions of likely punishments."[140] These fears are not borne out in reality. Using information from the Bureau of Justice Statistics' online Federal Criminal Case Processing Statistics Data Tool, the mean (or average) prison sentence for violations of section 1030(a) is below three years.[141] This is shown in Table 2 below, with 2022 being the most recent year for available records, and 2005 being the year in which the Sentencing Guidelines became advisory rather than mandatory.[142] The number of persons charged using section 1030 has decreased from a high of 149 in 2009 to only 51 in 2022.[143] This is not to minimize the impact of any custodial sentence, but to highlight the relatively low average prison sentence (i.e., under sixty months) imposed under section 1030, more notable because not everyone convicted was sentenced to prison: in 2022, fifteen defendants received probation only, while seventeen were sentenced to prison.[144]

138. Benjamin A. Soullier, *Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren*, 76 FED. COMM. L.J. 239 (2024).

139. Blair V. Robinson, *Cyber Sit-Ins; Bringing Protest Online by Modernizing the Computer Fraud and Abuse Act*, 28 ROGER WILLIAMS U. L. REV. 80, 81 (2023).

140. Orin S. Kerr, *Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases*, 84 GEO. WASH. L. REV. 1544, 1545 (2016).

141. *See* Statistics Data Tool, *supra* note 126 (following same instructions).

142. United States v. Booker, 543 U.S. 220, 233 (2005).

143. Statistics Data Tool, *supra* note 126 (following same instructions).

144. *Id.*

Table 2 Mean (Average) Prison Sentences for § 1030(a) Offenders

| Year | Sentence (months) |
|---|---|
| 2005 | 24.16 |
| 2006 | 58.17 |
| 2007 | 30.49 |
| 2008 | 25.27 |
| 2009 | 35.23 |
| 2010 | 33.90 |
| 2011 | 42.68 |
| 2012 | 31.80 |
| 2013 | 36.91 |
| 2014 | 33.81 |
| 2015 | 30.05 |
| 2016 | 37.63 |
| 2017 | 26.81 |
| 2018 | 47.88 |
| 2019 | 24.56 |
| 2020 | 40.41 |
| 2021 | 26.52 |
| 2022 | 35.33 |
| Overall Mean | 34.53 |

### *J. How Hard Should We Hit Computer Fraud Enterprise Offenders?*

What kind of sentence would be appropriate for a defendant in a computer fraud and abuse enterprise? This may be answered in part by a process of elimination. A mandatory minimum sentence, regardless of its length, may pose issues of over-punishment and result in charge-bargaining, where prosecutors who manage to get a cybercrime enterprise defendant into court allow a plea to a lesser offense as part of a plea agreement. While mandatory minimum sentences may be Congress's expression of the seriousness of an offense, they then remove discretion from judges to impose any alternative sentence "sufficient but not greater than" necessary to achieve the aims set out in the touchstone law of federal sentencing.[145] Alternatively, some circumstances of cybercrime merit a sentence above twenty years, specifically those with a foreseeable risk of death or serious bodily injury. This is not a

145. 18 U.S.C. § 3553(a).

hypothetical example. In 2020, a German woman needing urgent medical care died when she had to be redirected to a second hospital after the first was victimized by ransomware.[146]

Ransomware groups target healthcare and public health more than any other sector,[147] because these sectors are data-rich and willing to pay.[148] Hospitals are targets of ransomware gangs, as described in the Trickbot Group indictment[149] and other recent statements from the Department of Justice,[150] and attacking the ability of a hospital to function has a foreseeable risk of serious bodily harm and death. One study admitted the difficulty of quantifying the impact of ransomware on U.S. hospitals, but estimated that "from 2016 to 2021 . . . ransomware attacks killed between 42 and 67 Medicare patients."[151] Rather than a mandatory minimum or a maximum of less than twenty years, a term of years sentence up to life would serve several purposes. It would not discourage guilty pleas from defendants seeking to avoid a stiff mandatory minimum. It would not unduly cap a sentence where the conduct demands severe punishment. Finally, it would allow judges to do what they are supposed to do: weigh the conduct, the harm, the defendant's history and role in the offense, listen to the arguments of counsel, and arrive at a fair and just sentence.[152]

### *K. Features of the Proposed New Subsection*

Proposed language for a new "enterprise" subsection to section 1030 is included as an appendix herein. This is largely patterned on the RICO Act, but also includes a mens rea requirement of "knowingly," to prevent conviction of those who may be

146. *German hospital hacked, patient taken to another city dies*, AP NEWS (Sept. 17, 2020, 14:53 MST), https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94 [https://perma.cc/S4WQ-K9YW].

147. FBI, INTERNET CRIME REPORT 2023 13 (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

148. Jane Edwards, *FBI Report Reveals Top 3 Ransomware Targets in 2023* (Mar. 7, 2024), EXECUTIVEGOV, https://executivegov.com/2024/03/fbi-report-reveals-top-3-ransomware-targets-in-2023/ [https://perma.cc/TL6W-33BD].

149. Tsarev Indictment, *supra* note 49, ¶¶ 53, 55.

150. *See* Press Release, U.S. DEP'T OF JUST., Foreign National Pleads Guilty to Role in Cybercrime Schemes Involving Tens of Millions of Dollars in Losses (Feb. 15, 2024), https://www.justice.gov/archives/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars [https://perma.cc/WSL6-32CZ] (quoting Acting Assistant Attorney General Nicole M. Argentieri: "These criminal groups stole millions of dollars from their victims and even attacked a major hospital with ransomware, leaving it unable to provide critical care to patients for over two weeks.").

151. Hannah T. Neprash et al., *We tried to quantify how harmful hospital ransomware attacks are for patients. Here's what we found*, STAT (Nov. 17, 2023), https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/ [https://perma.cc/6NL3-KTU2].

152. 18 U.S.C. § 3553.

unknowingly employed in such an enterprise, as in the case of a low-level programmer. The proposed subsection also includes a damage threshold of $100,000, twenty times the threshold currently used in section 1030, again as a safeguard to prevent use against defendants committing lesser harms. Importantly, the subsection could be used against any person who is knowingly employed by or associated with a computer fraud and abuse enterprise, i.e., a malware or ransomware organization. The proposed addition does not require the person charged to have personally committed the felonious acts in section 1030 forming the basis of the enterprise, borrowing the concept from the CCE statute. These borders encompass the conduct seen in modern malware and ransomware groups, without the over-breadth likely to decrease support for such a change.

### *L. Back to the Pipeline: Differences in Sentencing Law*

Returning to the Colonial Pipeline incident, suppose a co-conspirator was apprehended, charged, and convicted in the United States. This is an unlikely scenario, but not an impossible one. DarkSide is the Russia-based group behind the Colonial Pipeline attack, with a $10 million reward still offered for information leading to identification of its leaders and $5 million for information leading to the arrest of any co-conspirator.[153] For the sake of comparison, only charges under the current and proposed modification of section 1030 will be used, with some follow-up on other charges likely to be brought. For purposes of the statute as it currently exists, assume the defendant is convicted under section 1030(a)(5), intentionally damaging a computer by knowing transmission of a program, information, code, or command, section 1030(a)(4), accessing a computer to defraud and obtain value, and section 1030(a)(7) extortion involving computers. The first charge is based on an impairment within a Colonial Pipeline computer, reportedly the one used for billing.[154] The relevant section of the U.S. Sentencing Guidelines is the one used for most crimes of fraud and financial loss, USSG § 2B1.1.[155]

Federal sentencing uses a grid-based system in which a point-value offense level is calculated using the Sentencing Guidelines

153. Press Statement, U.S. DEP'T OF STATE, Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice (Nov. 4, 2021), https://2021-2025.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ [https://perma.cc/F6BD-L5J3].

154. Ido Kilovaty, *Cybersecuring the Pipeline*, 60 HOU. L. REV. 605, 607–08 (2023).

155. U.S. SENT'G GUIDELINES MANUAL § 2B1.1 (Theft, Property Destruction, and Fraud) (U.S. SENT'G COMM'N 2024).

(vertical axis of the grid), and calculation of the defendant's prior criminal history category (horizontal axis of the grid) to yield a sentencing range in months.[156] That range is advisory, not mandatory, so a judge is free to vary from it in the absence of any mandatory minimum sentence.[157] Using USSG § 2B1.1(a)(2), the base offense level is 6, and the next task would be to determine the loss amount.[158] The ransom amount of approximately $4.4 million represents an actual loss, as the company paid the criminals, but the costs of remediation, or restoration of systems and data to its prior working condition, also count if they are reasonably foreseeable from the conduct.[159] For the sake of this hypothetical, assume the total loss is greater than $3.5 million but less than $9.5 million, resulting in an 18-level increase in the offense level, now up to 24.[160] While reports state that the ransomware attack first involved an exfiltration of personal data,[161] assume that this specific offense characteristic will not be applied to the facts of the conviction.[162] However, as the crime "caused a substantial disruption of critical infrastructure," the offense level is increased by 6, to a total of 30.[163] Because all three charges involve the same loss and conduct, there is no increase for multiple charges.[164] The resulting sentence in months, assuming no prior criminal history, is 97-121 months, or 70-87 months if the defendant received a three-point reduction for acceptance of responsibility (pleading guilty).[165] Under the Sentencing Guidelines, the court should impose a sentence of not more than 121 months, one month above the statutory maximum of the § 1030(a)(5)(A) count.[166] However, as the Sentencing Guidelines are advisory, the sentence could be a total of twenty years if all three counts were imposed at their statutory maximums and ran consecutively to each other. Such an upward

156. USSG Ch.5, Pt. A, sentencing table [hereinafter USSG Sentencing Table].

157. United States v. Booker, 543 U.S. 220, 246 (2005).

158. USSG § 2B1.1(a)(2).

159. *See, e.g.*, United States v. Cedeno, 471 F.3d 1193, 1194–95 (11th Cir. 2006).

160. USSG § 2B1.1(b)(1)(J).

161. Brian Fung, *Colonial Pipeline says ransomware attack also led to personal information being stolen*, CNN BUS., (Aug. 16, 2021, 13:10 EDT), https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html [https://perma.cc/3N3X-Y47B].

162. USSG § 2B1.1(b)(18).

163. *Id.* at § 2B1.1(b)(19)(A)(iii) (while §4B1.3, Criminal Livelihood, could apply, it would have no effect on these facts as it would only raise the total offense level to 13—absent a guilty plea).

164. *Id.* at § 3D1.1.

165. *See* USSG Sentencing Table, *supra* note 156; *see also* USSG § 3E1.1.

166. *See* USSG § 5G1.2(d) ("If the sentence imposed on the count carrying the highest statutory maximum is less than the total punishment, then the sentence imposed on one or more of the other counts shall run consecutively, but only to the extent necessary to produce a combined sentence equal to the total punishment.").

variance or departure from the Sentencing Guidelines range would require sufficient justification to be found reasonable if appealed.[167]

If a section 1030 "enterprise" subsection like the one suggested in the appendix were in effect, allowing any sentence up to life to be imposed, factors drawn from cybercrime's contemporary reality come into play. Those include consideration of relevant additional acts committed by the enterprise. While now nominally disbanded (but likely only rebranded), DarkSide victimized more organizations than the Colonial Pipeline Company. Cryptocurrency wallets attributable to DarkSide received at least $90 million before DarkSide disbanded, according to reports from analysts.[168] Even if similar acts were not charged, the court may consider the amount in the cryptocurrency wallets if the court found it represents relevant conduct.[169] That allows for a 24-level increase under the loss table of the Sentencing Guidelines, which is six levels higher than previously calculated under existing law.[170] While a court might apply the same relevant conduct rules under existing section 1030, it could exceed current statutory maximum penalties resulting from using that level of financial loss. For the proposed new subsection as described above, the resulting sentencing range is 188-235 months, or 135-168 if the defendant pleads guilty.[171] Those ranges are certainly more proportionate to the harm caused.

### *M. Why Change the Law?*

Critics might point out that using existing laws, such as wire fraud or the previous scenario of stacked section 1030 sentences, could yield a similar result. That assumption relies on a defendant being convicted of each count in an indictment, which is not a certainty. Moreover, the use of multiple charges puts the government to the burden of proving each element of each charge, no mean feat in matters of presenting highly technical evidence to a jury. Critics might also cite the potential for a sentence too severe, given the defendant's conduct. That ignores the advisory nature of

167. Gall v. United States, 552 U.S. 38, 39 (2007) ("In reviewing the sentence, the appellate court must first ensure that the district court made no significant procedural errors and then consider the sentence's substantive reasonableness under an abuse-of-discretion standard, taking into account the totality of the circumstances, including the extent of a variance from the Guidelines range, but must give due deference to the district court's decision that the [18 U.S.C.] § 3553(a) factors justify the variance.").

168. Ryan Browne, *Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down*, CNBC (May 18, 2021, 9:04 AM EDT), https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html [https://perma.cc/GPN4-RJPH].

169. *See* United States v. Cavallo, 790 F.3d 1202, 1232–35 (11th Cir. 2015).

170. USSG § 2B1.1(b)(1)(M).

171. USSG Sentencing Table, *supra* note 156; *see also* USSG § 3E1.1.

the guidelines and the ability of the prosecution and defense to enter into plea agreements, which guide or limit sentence length. An example is seen in the plea agreement of a defendant who committed violations of the CFAA affecting a hospital.[172] Employed by a computer security firm that served hospitals, the defendant hacked a hospital's phone systems used for internal communications, including 'code blue' emergencies.[173] He also obtained personal identity information of patients and released it on a social media site.[174] Despite that conduct, the government made a non-binding sentencing recommendation of 57 months of probation, largely based on the defendant having a terminal medical condition.[175] A new subsection for section 1030 with an indeterminate sentence up to life can cleanly address conduct of ransomware groups, with potential stiff sentences promoting deterrence but avoiding mandatory minimums for lesser conduct. The time to change this law is long overdue, and waiting any longer means that any defendant apprehended until such a change is made benefits from the existing scheme of using relatively low- to mid-punishment levels and substitute charges.

## CONCLUSION

Ransomware drains hundreds of millions of dollars from the U.S. economy[176] and leads directly to the deaths of Americans,[177] yet over ten years into the era of ransomware no changes to the only federal law addressing computer fraud and abuse have been made.[178] The CFAA's conspiracy provision is like a broken internet link pointing to a removed site, as it has no clear penalty provision, and jointly undertaken cybercrime activity is frequently charged using other statutes. An update targeting "kingpins" may fail to capture the way in which modern malware and ransomware organizations operate as a kind of "gig economy" of affiliates.[179] An

172. Guilty Plea and Plea Agreement, United States v. Vikas Singla, 692 F. Supp. 3d 1341 (N.D. Ga. 2023) (No. 1:21-cr-00228-MLB-RDC) [hereinafter Guilty Plea and Plea Agreement].

173. Connor Jones, *Former infosec COO pleads guilty to attacking hospitals to drum up business*, REGISTER (Nov. 20, 2023, 17:15 UTC), https://www.theregister.com/2023/11/20/former_infosec_coo_pleads_guilty/ [https://perma.cc/S5D2-4WW9].

174. *See* Guilty Plea and Plea Agreement, *supra* note 172, ¶ 12k.

175. *Id.* ¶ 18.

176. *See generally* CHAINALYSIS, *supra* note 39, at 5.

177. Neprash et al., *supra* note 151.

178. *See generally* Neal, *supra* note 35 (discussing a malware issue that occurred in 2013).

179. *Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself*, MICROSOFT (May 9, 2022), https://www.microsoft.com/en-

updated law to combat jointly-undertaken cybercrime activity would benefit from the existing definition of an enterprise seen in the RICO Act, but also from a monetary threshold in criminal proceeds and damages caused by criminal actors, as a gate-keeping function to prevent over-punishment of less culpable defendants. Such an update to the CFAA would benefit from excluding mandatory minimum punishment but also from allowing the maximum punishment to be up to life imprisonment, to both encourage guilty pleas on the charge and account for conduct up to that with a foreseeable risk of death. Without a timely update, the CFAA remains a suboptimal and anachronistic weapon against modern criminal organizations, akin to a cavalry charge against an armored unit. Even when coupled with general federal conspiracy law, potential sentences are too short given the harm done.[180] If post-Colonial Pipeline federal action included a fine on the victim corporation amounting to one-quarter of the extortionate demand of the criminals,[181] certainly an update to the CFAA is warranted to properly punish modern cybercriminals. The proposed subsection to section 1030 included in the appendix uses several features drawn from other "enterprise" laws while excluding others. The proposed subsection is potentially viable as it is drafted, but it may benefit from fine-tuning in the legislative process, so long as the result addresses jointly undertaken criminal activity as outlined above.

us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/ [https://perma.cc/36F4-5CPX].

180. 18 U.S.C. § 371.

181. *See* Notice to Colonial Pipeline, *supra* note 6.

## APPENDIX

A Suggestion for New Statutory Language Within § 1030:

It shall be unlawful for any person knowingly employed by or knowingly associated with any computer fraud and abuse enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs.

Any person who engages in a computer fraud and abuse enterprise shall be sentenced to a term of imprisonment in excess of one year and which may be up to life imprisonment, to a fine not to exceed the greater of that authorized in accordance with the provisions of Title 18 or $2,000,000 if the defendant is an individual or $5,000,000 if the defendant is other than an individual, and to the forfeiture prescribed in this section.

"Computer fraud and abuse enterprise" defined

For purposes of subsection a computer fraud and abuse enterprise exists where there is—

(1) a violation any provision of this section, the punishment for which is a felony, and

(2) such violation is a part of a series of violations of this section,

(3) resulting in

(a) proceeds to the enterprise, or

(b) damage to computers, or

(c) costs of remediation, or

(d) any combination of (a) – (c) above, in a total amount in excess of $100,000.

(4) "enterprise" includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.