Ransomware and Federal Law: Cybercrime and Cybersecurity

October 5, 2021

Congressional Research Service
https://crsreports.congress.gov
R46932

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Ransomware and Federal Law: Cybercrime and Cybersecurity

SUMMARY

R46932

October 5, 2021

Peter G. Berris
Legislative Attorney

Jonathan M. Gaffney
Legislative Attorney

Ransomware attacks—the use of malicious software to deny users access to data and information systems to extort ransom payments from victims—are prevalent. A recent notable example is the May 2021 ransomware attack that temporarily shut down the Colonial Pipeline Company's network, affecting gasoline availability and prices. This attack is but one of many; in 2020 alone, the Federal Bureau of Investigation (FBI) received nearly 2,500 ransomware complaints with losses exceeding $29 million.

Federal law provides several potential approaches to combat ransomware attacks. First, federal criminal laws, such as the Computer Fraud and Abuse Act (CFAA), can be used to prosecute those who perpetrate ransomware attacks. These laws and others, such as the statutes criminalizing conspiracy and aiding and abetting, might also be used to prosecute individuals who help to develop ransomware that is ultimately used by others. Victims who pay ransoms might also be subject to criminal or civil penalties in some cases—for example, where a ransom payment is made knowingly to an entity either designated as a foreign terrorist organization or subject to sanctions by the Department of Treasury. Nevertheless, policy considerations, mitigating factors, and prosecutorial discretion may weigh against enforcement in such instances.

Second, federal cybersecurity laws play an important role in both preventing and responding to ransomware attacks. Cyber preparedness laws require federal agencies to secure their networks and authorize the Cybersecurity and Infrastructure Security Agency (CISA) and Office of Personnel Management (OPM) to establish federal network security requirements. Other cyber preparedness laws authorize federal agencies to assist private entities operating in critical infrastructure sectors in securing their systems. Moreover, many data protection laws include requirements for covered entities to safeguard customer or consumer data. If a ransomware attack or other cyber incident occurs, federal law requires CISA and other federal agencies to work together to mitigate harm to federal networks and authorizes them to assist private entities in incident response and damage mitigation.

Contents

Contacts

Introduction

A series of high-profile cyberattacks[1] and the interruptions they caused have captured news headlines[2] and the attention of the Biden Administration,[3] federal law enforcement,[4] and Members of Congress.[5] The attacks have renewed focus on the problem of ransomware—malicious software (malware) generally used for extortion—that denies users access to their data and information systems.[6] Ransomware attackers generally demand payment, often in cryptocurrency, to make a victim's data accessible.[7] For example, in May 2021, a ransomware attack prompted the Colonial Pipeline Company to shut down its network temporarily, impacting gasoline availability and prices[8] before the company reportedly paid a ransom of over $4 million worth of Bitcoin.[9] Several weeks later, another ransomware attack on meat supplier JBS resulted in the shutdown of a number of meat processing plants in the United States and abroad.[10] The

[1] This report uses the terms "cyberattack," "cyber intrusion," and "cyber incident" interchangeably. Some laws or regulations may define these terms more or less specifically. *See, e.g.*, 6 U.S.C. § 1500(g)(2) (defining "cyber attack . . . of particular consequence); 44 U.S.C. § 3552(2) (defining "incident"); 50 U.S.C. § 3371c(a)(4) (defining "cyber intrusion"); PPD-41, PRESIDENTIAL POLICY DIRECTIVE—UNITED STATES CYBER INCIDENT COORDINATION (2016) (defining "cyber incident").

[2] *E.g.*, Taylor Telford et al., *Fuel Shortages Crop Up in Southeast, Gas Prices Climb After Pipeline Hack*, WASH. POST (Mar. 11, 2021), https://www.washingtonpost.com/business/2021/05/11/gas-shortage-colonial-pipeline/; Jacob Bunge, *Meat Buyers Scramble After Cyberattack Hobbles JBS*, WALL ST. J. (June 2, 2021), https://www.wsj.com/articles/meatpacker-jbs-hit-by-cyberattack-affecting-north-american-australian-operations-11622548864.

[3] *E.g.*, Elena Moore, *The White House Announces Additional Steps to Combat Ransomware*, NPR (July 15, 2021), https://www.npr.org/2021/07/15/1016224865/the-white-house-announces-additional-steps-to-combat-ransomware; Alex Marquardt & Geneva Sands, *First on CNN: White House pushes for companies to take ransomware more seriously after high-profile cyberattacks*, CNN (June 3, 2021), https://www.cnn.com/2021/06/03/politics/white-house-open-letter-ransomware-attacks-businesses/index.html.

[4] *E.g.*, Caroline Kenny & Pamela Brown, *Senate Sergeant-at-Arms Says Cyber Threat, Not Another Insurrection, Keeps Her Up at Night*, CNN (June 6, 2021), https://www.cnn.com/2021/06/04/politics/karen-gibson-senate-sergeant-at-arms-cyber-threat-insurrection-cnntv/index.html; Aruna Viswanatha & Dustin Volz, *FBI Director Compares Ransomware Challenge to 9/11*, WALL ST. J. (June 4, 2021), https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003?st=j7ayruzqxbcplzp&reflink=desktopwebshare_permalink.

[5] *E.g.*, *America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (Jul. 27, 2021); *Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis: Hearing before the H. Comm. on Homeland Sec.*, 117th Cong. (May 5, 2021); Maggie Miller, *Lawmakers Roll Out Legislation to Defend Pipelines Against Cyber Threats*, THE HILL (May 14, 2021), https://thehill.com/policy/cybersecurity/553598-lawmakers-roll-out-legislation-to-defend-pipelines-against-cyber-threats.

[6] CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran; *Scams and Safety: Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (last visited Sept. 29, 2021).

[7] U.S. DEP'T OF THE TREASURY, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 1-2 (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[8] Parfomak & Jaikaran, *supra* note 6; *see generally* Stephanie Kelly & Laura Sanicola, *U.S. Capital Running Out of Gas, Even as Colonial Pipeline Recovers*, REUTERS (May 14, 2021), https://www.reuters.com/business/energy/colonial-pipeline-ramps-up-us-seeks-emerge-fuel-crunch-2021-05-14/; Brett Molina & Nathan Bomey, *Colonial Pipeline Restarted Operations, Owners Say "It Will Take Several Days" For Supply Chain to Return to Normal*, USA TODAY (May 12, 2021), https://www.usatoday.com/story/money/2021/05/12/gas-shortage-gas-prices-colonial-pipeline-nc-virginia-north-carolina/5052551001/; Catherine Thorbecke, *Gas Hits Highest Price in 6 Years, Fuel Outages Persist Despite Colonial Pipeline Restart*, ABC NEWS (May 17, 2021), https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outages-persist/story?id=77735010.

[9] Cathy Bussewitz, *Colonial Pipeline Confirms It Paid $4.4M to Hackers*, AP NEWS (May 19, 2021), https://apnews.com/article/hacking-technology-business-ed1556556c7af6220e6990978ab4f745.

[10] Hamza Shaban et al., *JBS, World's Biggest Meat Supplier, Says Its Systems Are Coming Back Online After*

company ultimately paid a ransom amounting to roughly $11 million in Bitcoin.[11] The problem has not been limited to these high-profile incidents: other notable ransomware attacks have reportedly targeted a brewing company,[12] major cities,[13] universities,[14] and health services providers,[15] among others.[16] In 2020, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) "received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million."[17] That figure is likely under-inclusive, as many ransomware attacks go unreported.[18]

This report explores legal issues implicated by two potential approaches to combatting ransomware. First, the report summarizes the potential for criminal prosecution under federal statutes such as the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA). This section of the report also discusses legal issues facing ransomware victims—in particular, whether victims risk legal liability by making ransomware payments. Second, the report summarizes federal laws governing public and private sector cybersecurity, including preparedness and incident response. This report does not cover technological and policy considerations involving ransomware, as these topics may be found in other CRS products.[19]

Cyberattack Shut Down Plants in U.S., WASH. POST (June 1, 2021), https://www.washingtonpost.com/business/2021/06/01/jbs-cyberattack-meat-supply-chain/; Julie Creswell et al., *Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business*, N.Y. TIMES (June 3, 2021), https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.

[11] Kevin Collier, *Beef Supplier JBS Paid Ransomware Hackers $11 Million*, NBC NEWS (June 9, 2021), https://www.nbcnews.com/tech/security/meat-supplier-jbs-paid-ransomware-hackers-11-million-n1270271; Aishwarya Nair, *Meatpacker JBS Says It Paid Equivalent of $11 Mln in Ransomware Attack*, REUTERS (June 10, 2021), https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/.

[12] *See e.g.*, Associated Press, *REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says*, NPR (June 3, 2021), https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says (giving Molson Coors as example of food company targeted by ransomware attackers).

[13] *See, e.g.*, Emily Sullivan, *Ransomware Cyberattacks Knock Baltimore's City Services Offline*, NPR (May 21, 2019), https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline (reporting ransomware attack on city of Baltimore); Stephen Deere, *Cost of City of Atlanta's Cyber Attack: $2.7 Million — and Rising*, ATLANTA J. CONST. (Apr. 12, 2018), https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI/ (detailing costs of ransomware attack on city of Atlanta).

[14] *See, e.g.*, Emily Sullivan, *Michigan State University Won't Pay Ransom After Cyber Attack*, M LIVE (June 3, 2020), https://www.mlive.com/news/2020/06/michigan-state-university-wont-pay-ransom-after-cyber-attack.html (discussing ransomware attack on Michigan State University); Associated Press, *University of Utah Pays $450K to Stop Cyberattack on Servers*, USA TODAY (Aug. 22, 2020), https://www.usnews.com/news/best-states/utah/articles/2020-08-22/university-of-utah-pays-450k-to-stop-cyberattack-on-servers (noting ransom paid to end ransomware attack on University of Utah).

[15] *E.g.*, Mike Snider, *Ransomware Hack Cripples Universal Health Services Hospitals, Facilities Across the US*, USA TODAY (Sept. 28, 2020), https://www.usatoday.com/story/tech/2020/09/28/health-care-provider-united-health-services-hit-cyberattack/3565533001/.

[16] *See, e.g.*, *Impact of Ransomware Attack on Mass. Steamship Authority Expected to Continue Thursday*, NBC BOSTON (June 2, 2021), https://www.nbcboston.com/news/local/mass-steamship-authority-delayed-due-to-cyber-attack/2395477/ (reporting ransomware attack on the Steamship Authority of Massachusetts).

[17] FBI, INTERNET CRIME REPORT 2020 14 (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[18] *See America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (July 27, 2021) (statement of Bryan A. Vorndran, Assistant Director of FBI Cyber Division) [hereinafter Vorndran Statement], available at https://www.judiciary.senate.gov/imo/media/doc/Vorndran - Statement.pdf#page=7 ("[R]ansomware incidents are often addressed by the victim directly and are never reported to the public or law enforcement.").

[19] *E.g.*, Parfomak & Jaikaran, *supra* note 6; CRS In Focus IF10559, *Cybersecurity: A Primer*, by Chris Jaikaran; CRS Insight IN11683, *Critical Infrastructure Policy: Information Sharing and Disclosure Requirements After the Colonial*

Federal Criminal Prosecution for Ransomware Attacks

Federal law criminalizes ransomware attacks.[20] One applicable statute is the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030—a civil and criminal cybercrime law that prohibits a range of computer-based activities.[21] Often described as the preeminent federal anti-hacking law,[22] the CFAA protects a broad range of computers and computerized devices, and the U.S. Department of Justice (DOJ) has used it to bring charges in the ransomware context.[23]

Depending on the nature of a ransomware attack, and of the targeted computers, various CFAA provisions could be relevant.[24] The archetypal ransomware attack—where an individual uses malware to encrypt files until a ransom is paid for decryption[25]—will probably violate § 1030(a)(7)(C),[26] which governs certain extortive threats involving computers.[27] Specifically, that provision makes it a crime to transmit in interstate or foreign commerce a demand for money or anything else of value "in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."[28] At a minimum, "protected computers" include all those connected to the internet,[29] and "damage" encompasses malware such as ransomware that impairs a computer—for example by causing it to "no longer operate[] . . . in response to the commands of the owner."[30]

Pipeline Attack, by Brian E. Humphreys.

[20] COMPUT. CRIME & INTELL. PROP. SECTION, U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES 54 (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (describing application of federal criminal law to instances where a cybercriminal "access[es] the victim's computer system, encrypts data, and then demand[s] money for the decryption key").

[21] CRS Report R46536, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, by Peter G. Berris, at 1.

[22] *E.g.*, Ivan Evtimov et al., *Is Tricking A Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019) ("Since its implementation, the CFAA has been the nation's predominant anti-hacking law.").

[23] *E.g.*, Indictment, United States v. Levashov, No. 3:17-cr-83-RNC, 2017 WL 8944387 (D. Conn. Apr. 20, 2017); Press Release, U.S. Dep't of Just., Alleged Operator of Kelihos Botnet Extradited From Spain (Feb. 2, 2018), https://www.justice.gov/opa/pr/alleged-operator-kelihos-botnet-extradited-spain; Press Release, U.S. Dep't of Just., Latvian National Charged for Alleged Role in Transnational Cybercrime Organization (June 4, 2021), https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization.

[24] *See* Berris, *supra* note 21, at n.190 (describing provisions ransomware attacks may violate).

[25] Parfomak & Jaikaran, *supra* note 6.

[26] U.S. DEP'T OF JUST., *supra* note 20. DOJ has used § 1030(a)(7)(C) to charge alleged ransomware attackers. *E.g.*, Indictment, United States v. Savandi, No. 3:18-cr-00704-BRM, 2018 WL 6798078 (D.N.J. Nov. 27, 2018); Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[27] 18 U.S.C. § 1030(a)(7)(C).

[28] *Id.*

[29] *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (interpreting the definition of protected computer in the context of one subsection of the CFAA to include "all computers that connect to the Internet"); hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019) ("The term 'protected computer' refers to any computer 'used in or affecting interstate or foreign commerce or communication,' . . . effectively any computer connected to the Internet . . . including servers, computers that manage network resources and provide data to other computers." (quoting 18 U.S.C. § 1030(e)(2)(B)) (internal citations omitted)).

[30] United States v. Yücel, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015) (construing damage under § 1030(a)(5) to include instances where a computer is caused to "no longer operate[] only in response to the commands of the owner"); *see*

In addition to encrypting files with ransomware, cybercriminals may also attempt to extort money by breaching a computer system, stealing sensitive information, and threatening to disclose that information if ransom is not paid.[31] Sometimes described as "double extortion,"[32] such schemes likely implicate § 1030(a)(7)(B), a CFAA provision which criminalizes:

- threats to obtain information through unauthorized access to a protected computer; and
- threats to disclose information already obtained through unauthorized access into a protected computer.[33]

Violations of both subsections of § 1030(a)(7) are felonies, punishable by fines and up to five years of imprisonment for first offenses, and ten years for subsequent offenses.[34] Depending on the circumstances, DOJ may also prosecute ransomware attackers under other CFAA subsections, such as provisions prohibiting trespass into government computers (§ 1030(a)(3)) or criminalizing various actions causing intentional damage to protected computers (§ 1030(a)(5)).[35] The CFAA also contains asset forfeiture provisions which may provide DOJ an opportunity to recover ransom payments and other illicitly obtained property.[36]

Other federal statutes could be relevant as well. For example, DOJ has charged ransomware attackers and developers with conspiracy to violate the federal wire fraud statute,[37] which criminalizes certain fraudulent schemes involving interstate wires.[38] Further, double extortion ransomware attacks may violate other statutes depending on the nature of the information stolen. The Economic Espionage Act (EEA)[39] authorizes criminal penalties for theft of trade secrets, including intangible "financial, business, scientific, technical, economic, or engineering information" that the owner "has taken reasonable measures to keep . . . secret" and that "derives independent economic value" from "not being generally known."[40] With certain limitations, the EEA makes it a crime to steal or misappropriate trade secrets:

---

also United States v. Hutchins, 361 F. Supp. 3d 779, 794 (E.D. Wis. 2019) (concluding that use of the phrase "malware" in indictment was "sufficient to allege intent to cause damage" in CFAA prosecution). For a more detailed examination of different examples of damage, *see, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW 31, 107-08 (3d ed. 2013).

[31] Vorndran Statement, *supra* note 18, at 2.

[32] *Id.*

[33] 18 U.S.C. § 1030(a)(7)(B). For additional analysis of this subsection, see Berris, *supra* note 21, at 18.

[34] 18 U.S.C. § 1030(c). For a detailed overview of CFAA penalties, see Berris, *supra* note 21, tbls. 1-4.

[35] An overview of these provisions are available at Berris, *supra* note 21, at 10-11, 14-16; *see also* Indictment, United States v. Vachon-Desjardins, No. 8:20-cr-366 (M.D. Fla. Dec. 2, 2020), available at https://www.justice.gov/usao-mdfl/press-release/file/1360846/download (charging ransomware defendant with violating § 1030(a)(5), among other provisions).

[36] 18 U.S.C. § 1030(j).

[37] Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public; Press Release, U.S. Dep't of Just., Latvian National Charged for Alleged Role in Transnational Cybercrime Organization (June 4, 2021), https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization.

[38] 18 U.S.C. § 1343. For additional legal analysis of § 1343, see generally CRS Report R41930, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law*, by Charles Doyle.

[39] CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, by Charles Doyle.

[40] 18 U.S.C. §§ 1831, 1832, 1839(3).

- with the intent or knowledge that they "will benefit any foreign government," instrumentality, or agent;[41] or
- for economic benefit, if the trade secrets relate to "a product or service used in or intended for use in interstate or foreign commerce."[42]

Although it is unclear if DOJ has used the EEA to prosecute ransomware attackers specifically,[43] federal prosecutors have used the EEA to charge defendants in connection with other types of cybercrimes.[44]

Criminal Enforcement of Ransomware Development

Beyond the immediate perpetrators of an attack, ransomware crimes involve malware developers and purveyors (although perpetrators may also be developers).[45] For example, one concern is the Ransomware-as-a-Service (RaaS) model "wherein certain criminals develop the malware and then sell or lease the tool to others to carry out ransomware campaigns" and share in the resulting criminal proceeds.[46] Such conduct may violate 18 U.S.C. § 1030(a)(5).[47]

In addition, inchoate offenses, such as conspiracy (18 U.S.C. § 371), provide another option for prosecuting ransomware developers.[48] Ordinarily a defendant is guilty of conspiracy if (1) he has agreed to commit a specific offense with at least one other person; (2) he knowingly participated in the conspiracy while intending to commit that offense; and (3) a conspirator commits an overt act in furtherance of the conspiracy.[49] DOJ has relied on these laws, and others like the aiding and abetting statute (18 U.S.C. § 2), in prosecuting a number of individuals for selling or developing various types of malware such as ransomware.[50] Prosecutors may find it difficult to establish

[41] *Id.* § 1831(a).

[42] *Id.* § 1832(a).

[43] For example, as of October 4, 2021, a search of justice.gov/news for press releases using the terms "ransomware" and "economic espionage" yielded no responsive results. Similarly, a search of the Westlaw database for cases citing 18 U.S.C. §§ 1831, 1832 and using the word "ransomware" returned no results.

[44] *E.g.*, CRS Legal Sidebar LSB10417, *Red Army Equifax Hackers Indicted*, by Charles Doyle.

[45] *See, e.g.*, Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public (describing indictment of defendants accused of authoring *and* deploying ransomware).

[46] CRS Insight IN11698, *Department of Justice Efforts to Counter Ransomware*, by Kristin Finklea.

[47] *See* discussion *supra* in "Federal Criminal Prosecution for Ransomware Attacks." For an overview of § 1030(a)(5) see Berris, *supra* note 21, at 14-16.

[48] 18 U.S.C. § 371. For additional legal analysis of § 371 see CRS Report R41223, *Federal Conspiracy Law: A Brief Overview*, by Charles Doyle.

[49] *E.g.*, United States v. Smith, 950 F.3d 893, 895 (D.C. Cir. 2020).

[50] For instance, prosecutors charged a member of a North Korean hacking team for conspiracy to violate CFAA provisions such as § 1030(a)(5) in connection with a scheme that involved developing the ransomware known as WannaCry2.0. Press Release, U.S. Dep't of Just., North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and; Criminal Complaint, United States v. Park Jin Hyok, No. MJ18-1479 (C.D. Cal. June 8, 2018). As another example, federal prosecutors charged one individual under § 1030(a)(5), among other offenses, in connection with his "creation and distribution of the Kronos banking Trojan and UPAS kit malware." First Superseding Indictment, United States v. Hutchins, No. 2:17CR00124, 2018 WL 7325296 (E.D. Wis. June 5, 2018); Press Release, U.S. Dep't of Just., Marcus Hutchins Pleads Guilty to Creating and Distributing the Kronos Banking Trojan and UPAS Kit Malware (May 3, 2019), https://www.justice.gov/usao-edwi/pr/marcus-hutchins-pleads-guilty-creating-and-distributing-kronos-banking-trojan-and-upas. Prosecutors also used § 1030(a)(5), along with other provisions, to charge a Swedish national responsible for

criminal intent in the case of some types of tools used to commit cybercrimes (such as botnets) because purveyors of those tools may be unaware of their eventual use.[51] Prosecutors may find it less onerous to show criminal intent in RaaS crimes because developers apparently intend the tools to aid in, and profit from, ransomware attacks.[52]

Criminal Enforcement of Ransomware Attacks from Abroad

The applicability of statutes like the CFAA to ransomware attacks may be restricted less by their scope, and more by external, practical considerations. In large part, this is because ransomware attacks—and other cybercrimes—often originate overseas.[53] Although DOJ has used the CFAA, EEA, and the wire fraud statute to charge individuals for cyberattacks originating in other countries,[54] obtaining convictions for such conduct can be difficult.[55] As another CRS product explains in detail, investigating and prosecuting criminal conduct in other countries raises questions of national sovereignty and may involve significant legal, practical, and diplomatic obstacles.[56] The United States lacks extradition treaties with some countries, which may make domestic prosecution of cybercriminals residing in those countries challenging, although not impossible.[57]

DOJ may also be able to use civil asset forfeiture—a statutory regime enabling DOJ to file lawsuits against certain property when involved in various crimes—to recover ransom payments

---

the sale of malware to "thousands of people in more than 100 countries." United States v. Yücel, 97 F. Supp. 3d 413, 416 (S.D.N.Y. 2015); Press Release, U.S. Dep't of Just., Swedish Co-Creator Of "Blackshades" Malware That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers Sentenced To 57 Months In Prison (June 23, 2015), https://www.justice.gov/usao-sdny/pr/swedish-co-creator-blackshades-malware-enabled-users-around-world-secretly-and-remotely.

[51] *See* Berris, *supra* note 21, at 26-29.

[52] *See* Finklea, *supra* note 46 (explaining that with RaaS, both the "developer and attacker . . . receive portions of the criminal proceeds").

[53] Vorndran Statement, *supra* note 18, at 5 ("We know our most significant threats come from foreign actors using global infrastructure to compromise U.S. networks.").

[54] *See*, *e.g.*, Press Release, U.S. Dep't of Just., Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy (Aug. 26, 2020), https://www.justice.gov/opa/pr/ghanaian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business-email (discussing extradition of Ghanaian citizen for trial in connection with "an indictment charging him with wire fraud, money laundering, computer fraud and aggravated identity theft"); Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (providing update on prosecution of Chinese national for wire fraud, EEA, and CFAA violations); Press Release, U.S. Dep't of Just., U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018), https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (giving overview of prosecution of Russian intelligence officers for wire fraud, CFAA violations, and aggravated identity theft, among other charges); Press Release, U.S. Dep't of Just., Romanian National "Guccifer" Extradited to Face Hacking Charges (Apr. 1, 2016), https://www.justice.gov/opa/pr/romanian-national-guccifer-extradited-face-hacking-charges (announcing extradition of Romanian man to face indictment alleging, among other things, cyberstalking, wire fraud, and CFAA violations).

[55] *See generally* Doyle, *supra* note 44 (discussing complications in prosecuting international cybercrime defendants); *see also* Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 173-83 (Feb. 14, 2018) (providing overview of challenges in prosecuting CFAA offenses originating abroad).

[56] CRS Report 94-166, *Extraterritorial Application of American Criminal Law*, by Charles Doyle, at 23.

[57] *Id.* at 31. For a detailed overview of extradition law, see generally CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Contemporary Treaties*, by Michael John Garcia and Charles Doyle.

made to cybercriminals in foreign countries.[58] DOJ used this authority in June 2021 to obtain a warrant to seize Bitcoin that Colonial Pipeline paid to ransomware attackers.[59]

Legality of Ransom Payments

While the illegality of ransomware attacks is relatively straightforward, ransomware victims face more nuanced legal issues when deciding whether to make ransomware payments. No federal statutes expressly criminalize making ransom or ransomware payments.[60] However, federal laws heavily restrict transactions with certain parties and could implicitly make ransomware payments to such parties a crime.[61] For example, one of the federal material support of terrorism statutes prohibits conduct such as knowingly providing currency or other property to entities designated by the Secretary of State as foreign terrorist organizations.[62] At least theoretically, an individual might incur criminal penalties under the statute for making a ransomware payment to a recipient that he knows is a foreign terrorist organization. As another example, in a September 2021 advisory, the Treasury Department explained that federal regulations prohibit ransomware payments to individuals or entities on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List (SDN List) or those "covered by comprehensive country or region embargoes."[63] The Treasury Department stated that such payments could be subject to civil enforcement;[64] and, if an individual is aware that such a ransomware payment is unlawful—for example, if he knows that the recipient is on the SDN List or otherwise subject to embargo—then making that payment may incur criminal penalties.[65]

Nevertheless, policy considerations, mitigating factors, and prosecutorial discretion may weigh against criminal prosecution for ransomware payments even when they are knowingly made to sanctioned entities or foreign terrorist organizations.[66] In the context of hostage-taking, for example, DOJ clarified in 2015 that it "has never used the material support statute to prosecute a hostage's family or friends for paying a ransom for the safe return of their loved one."[67] To

[58] *See generally* CRS Report 97-139, *Crime and Forfeiture*, by Charles Doyle.

[59] See Press Release, U.S. Dep't of Just., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (announcing recovery of cryptocurrency paid as ransom in Colonial Pipeline incident and attaching warrants and affidavits listing legal authority to seize that cryptocurrency).

[60] For instance, 18 U.S.C. § 875 criminalizes certain ransom demands, but does not prohibit ransom or ransomware payments. 18 U.S.C. § 875.

[61] *See infra* notes 62-65 and accompanying discussion.

[62] 18 U.S.C. § 2339B; CRS Report R46829, *Domestic Terrorism: Overview of Federal Criminal Law and Constitutional Issues*, by Peter G. Berris, Michael A. Foster, and Jonathan M. Gaffney, at 7-9.

[63] U.S. DEP'T OF THE TREASURY, *supra* note 7, at 3.

[64] *Id.* at 4.

[65] For example, two different federal statutes impose criminal penalties for willful violations of various federal sanctions laws and regulations. 50 U.S.C. §§ 1705(c), 4315(a). Courts have generally interpreted "willfulness" under these statutes to require knowledge on the part of the defendant that his conduct was unlawful. *E.g.*, United States v. Mousavi, 604 F.3d 1084, 1094 (9th Cir. 2010); United States v. Homa Int'l Trading Corp., 387 F.3d 144, 146 (2d Cir. 2004); United States v. Dien Duc Huynh, 246 F.3d 734, 741-42 (5th Cir. 2001).

[66] For example, the Treasury Department has listed several mitigating factors that OFAC will consider in determining whether to enforce sanctions laws against an entity that makes an illegal ransomware payment, including the extent to which that entity disclosed the ransomware attack and payment, cooperated with law enforcement, and has employed cybersecurity measures to prevent ransomware attacks. U.S. DEP'T OF THE TREASURY, *supra* note 7, at 4-5.

[67] Press Release, U.S. Dep't of Just., Department of Justice Statement on U.S. Citizens Taken Hostage Abroad (June

combat ransomware, some have argued that Congress should remove the profit motive for ransomware attacks by criminalizing or otherwise prohibiting ransomware payments.[68] The issue has garnered media attention[69] and sparked a policy debate.[70] At a July 2021 Senate Judiciary Committee hearing, one FBI official stated that the Bureau does not support a ban on ransomware payments out of concern that it would make it possible for ransomware attackers to engage in a new form of extortion—specifically, the blackmailing of entities who make ransomware payments in violation of a ban.[71] Legislatures in at least four states are considering bills that would prohibit state or local government from making ransomware payments or from using public money to do so.[72] Further, a proposed bill in New York would authorize civil penalties of up to $10,000 for governmental, business, or health care entities that make a ransomware payment.[73]

Federal Cybersecurity Laws

In addition to the criminal provisions discussed above, federal law plays an important role in preventing and responding to ransomware and other cyberattacks.[74] Federal cybersecurity law

24, 2015), https://www.justice.gov/opa/pr/department-justice-statement-us-citizens-taken-hostage-abroad.

[68] Ben Kamisar, *Energy Secretary Backs Ban on Ransomware Payments: "You Are Encouraging the Bad Actors"*, NBC NEWS (June 6, 2021), https://www.nbcnews.com/politics/meet-the-press/sec-granholm-backs-ban-ransomware-payments-you-are-encouraging-bad-n1269776; Jason Breslow, *How to Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims from Paying Up*, NPR (May 13, 2021), https://www.npr.org/2021/05/13/996299367/how-to-stop-ransomware-attacks-1-proposal-would-prohibit-victims-from-paying-up; Robert K. Knake, *Paying Ransom on Ransomware Should Be Illegal*, COUNCIL ON FOREIGN RELS. (Feb. 29, 2016), https://www.cfr.org/blog/paying-ransom-ransomware-should-be-illegal.

[69] *E.g.*, Joe Tidy, *Ransomware: Should Paying Hacker Ransoms Be Illegal?*, BBC NEWS (May 20, 2021), https://www.bbc.com/news/technology-57173096; Joel Cohen, *Succumbing to Ransomware: There's No Federal Law Against It*, BLOOMBERG L. (June 14, 2021), https://news.bloomberglaw.com/us-law-week/succumbing-to-ransomware-theres-no-federal-law-against-it; Scott Tong, *As Ransomware and Other Cyberattacks Grow, Cyber Insurance Struggles to Keep Up*, MARKETPLACE (June 3, 2021), https://www.marketplace.org/2021/06/14/as-ransomware-and-other-cyberattacks-grow-cyber-insurance-struggles-to-keep-up/.

[70] *See, e.g.*, Alvaro Marañon & Benjamin Wittes, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021), https://www.lawfareblog.com/ransomware-payments-and-law ("At a minimum, Congress should consider banning ransomware payments made without notice both to authorities and to shareholders."); INST. FOR SEC. & TECH. RANSOMWARE TASKFORCE, COMBATTING RANSOMWARE 49 (2021) ("[T]he Ransomware Task Force did not reach consensus on prohibiting ransom payments, though we do agree that payments should be discouraged as far as possible."); Kyle Balluck, *Warner: Debate on Making It Illegal to Pay Ransoms "Worth Having"*, THE HILL (June 6, 2021), https://thehill.com/policy/cybersecurity/557040-warner-debate-on-making-it-illegal-to-pay-ransoms-worth-having (surveying debate over ransomware ban); Edward Segal, *Banning Ransomware Payments Could Create New Crisis Situations*, FORBES (June 8, 2021), https://www.forbes.com/sites/edwardsegal/2021/06/08/banning-ransomware-payments-could-create-new-crisis-situations/?sh=39580f502982 (examining possible business consequences of ransomware ban); Editorial Board, *Opinion: Hackers Are Taking Cities Hostage. Here's a Way Around It*, WASH. POST (June 23, 2019), https://www.washingtonpost.com/opinions/hackers-are-taking-cities-hostage-heres-a-way-around-it/2019/06/23/f08b79ea-9459-11e9-aadb-74e6b2b46f6a_story.html (advocating for ransomware ban).

[71] *See America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (Jul. 27, 2021) (testimony of Bryan Vorndran) ("It would be our opinion that if we banned ransom payments, now you're putting U.S. companies in a position to face yet another extortion, which is being blackmailed for paying the ransom and not sharing that with the authorities.").

[72] *E.g.*, H.R. 813, Gen. Assemb., 2021 Sess. (N.C. 2021); S. 6154, 2021 State Assemb., Reg. Sess. (N.Y. 2021); S. 726, Gen. Assemb., 2021 Sess. (Pa. 2021); H.R. 3892, Leg., 87(R) Sess. (Tex. 2021).

[73] S. 6806, 2021 State Assemb., Reg. Sess. (N.Y. 2021).

[74] For additional background on federal cybersecurity, see CRS Report R46926, *Federal Cybersecurity: Background and Issues for Congress*, by Chris Jaikaran.

generally does not distinguish between ransomware and other types of cyber threats; accordingly, this section describes federal cybersecurity laws more broadly. First, federal *cyber preparedness* laws authorize creating federal agency cybersecurity requirements, define federal agencies' roles in safeguarding critical infrastructure, and create sector-specific data protection requirements. In furtherance of these laws, federal agencies publish mandatory and voluntary guidelines, identify best practices, and provide tools for preventing cyber intrusions. If cyber intrusions occur, other federal laws direct how federal agencies and other entities respond to and mitigate those attacks. These laws can include mandatory reporting requirements and penalties for failing to comply with preparedness obligations.

Two recently created agencies play a notable coordinating role in federal cyber policy. Since its establishment in 2018,[75] the Cybersecurity and Infrastructure Security Agency (CISA) has taken a lead role in coordinating federal cybersecurity activities, with a mission that includes "lead[ing] efforts to protect the federal '.gov' domain of civilian government networks" and "collaborat[ing] with the private sector—the '.com' domain—to increase the security of critical networks."[76] In 2020, Congress created a new agency within the Executive Office of the President, the Office of the National Cyber Director, to advise the president on cybersecurity and coordinate the implementation of the National Cyber Strategy.[77] In May 2021, President Biden nominated Chris Inglis to be the first National Cyber Director;[78] the Senate confirmed the nomination on July 17.[79]

Cybersecurity Preparedness

Federal laws governing cybersecurity preparedness generally fall into three categories: (1) federal network security; (2) critical infrastructure protection; and (3) data protection and privacy.

Federal Network Security

Pursuant to the Federal Information Security Modernization Act (FISMA),[80] each federal agency is responsible for its own information security under the guiding principle that the level of protection for a system should be "commensurate with the risk and magnitude of the harm resulting from" a breach of that system.[81] For federal networks other than defense, intelligence, and national security systems, the U.S. Department of Homeland Security (DHS), through CISA, and the Office of Management and Budget (OMB) work together to implement cybersecurity policies,[82] guided by standards developed by the National Institute of Standards and

[75] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168.

[76] *Cybersecurity Mission and Vision*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cybersecurity-division (last visited Sept. 28, 2021). For more information about CISA and its federal cybersecurity role, see CRS In Focus IF10683, *DHS's Cybersecurity Mission—An Overview*, by Chris Jaikaran.

[77] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388; *see* John Costello & Mark Montgomery, *How the National Cyber Director Position is Going to Work: Frequently Asked Questions*, LAWFARE (Feb. 24, 2021), https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions.

[78] Michael D. Shear & Julian E. Barnes, *Biden Names N.S.A. Veteran to Be First National Cyber Director*, N.Y. TIMES (Apr. 12, 2021), https://www.nytimes.com/2021/04/12/us/politics/chris-inglis-cyber-director.html.

[79] Presidential Nomination 455, 117th Cong. (2021) (confirmed June 17, 2021).

[80] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

[81] 44 U.S.C. § 3554(a)(1)(A).

[82] *Id.* § 3553; 40 U.S.C. § 11331(b).

Technology.[83] As part of this mission, the DHS Secretary has the authority to issue binding directives on federal agencies.[84] For example, DHS's most recent binding directive requires federal agencies to develop a vulnerability disclosure policy to guide individuals in how to report security vulnerabilities in an agency's systems.[85]

To supplement these policies, CISA must, among other duties, provide training and security resources to federal agencies, including intrusion detection and protection systems and advanced network security tools.[86] CISA must also provide cyber threat analyses, assess and monitor agencies' cyber preparedness, and develop a comprehensive national cybersecurity plan.[8788] These laws likely would require CISA to share analyses of ransomware threats and help agencies develop plans to recover from ransomware attacks.

National security systems, such as some systems operated by the Department of Defense or the intelligence community, follow a different cybersecurity regime.[89] Each agency that operates or controls a national security system is responsible for securing that system consistent with presidential guidance.[90] For these systems, the Secretary of Defense or Director of National Intelligence has the authority of the OMB Director in developing and implementing information security standards.[91]

Critical Infrastructure Protection

Beyond the federal networks, federal law authorizes various agencies to develop and share resources to protect the nation's critical infrastructure (CI) sectors, defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[92] As designated

[83] 15 U.S.C. § 278g-3.

[84] 44 U.S.C. § 3553(b)(2); *see Cyber Directives*, U.S. DEP'T OF HOMELAND SEC., https://cyber.dhs.gov/directives/ (last visited Sept. 28, 2021).

[85] U.S. DEP'T OF HOMELAND SEC., BINDING OPERATIONAL DIRECTIVE 20-01: DEVELOP AND PUBLISH A VULNERABILITY DISCLOSURE POLICY (2020).

[86] *See* 6 U.S.C. §§ 652(c)(11) (requiring, among other things, the CISA Director to "provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security"), 663 (requiring DHS to "deploy, operate, and maintain" a federal intrusion detection and prevention system), 1522 (requiring DHS to "include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools").

[87] CISA provides public alerts regarding ransomware attacks and preparedness. *See Nat'l Cyber Awareness Sys – Alerts*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://us-cert.cisa.gov/ncas/alerts (last visited Oct. 2, 2021).

[88] *Id.* §§ 652(e)(1)(E) (requiring CISA to develop "a comprehensive national plan for securing the key resources and critical infrastructure of the United States"), 655 (requiring CISA to provide "analysis and warnings related to threats to, and vulnerabilities of, critical information systems"); 44 U.S.C. § 3553(b)(3) (requiring DHS to "monitor[] agency implementation of information security policies and practices"), (b)(6)(D) (requiring DHS to "develop[] and conduct[] targeted operational evaluations, including threat and vulnerability assessments, on [federal] information systems").

[89] A *national security system* is "any information system . . . used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency" for intelligence, national security, military, or other classified activities, excluding some systems "used for routine administrative and business applications." *Id.* § 3552(6).

[90] *Id.* § 3557.

[91] *Id.* § 3553(d)-(e).

[92] 42 U.S.C. § 5195c.

most recently by Presidential Policy Directive 21 (PPD-21),[93] there are sixteen CI sectors, including communications, emergency services, and financial services.[94] Each CI sector has a corresponding *sector risk management agency*: a federal department or agency that (1) provides institutional knowledge and specialized expertise; and (2) coordinates implementation of federal cyber policy with respect to its assigned sector.[95] CISA and the sector risk management agencies share responsibility for developing cybersecurity standards for and providing assistance to CI sectors.[96] In addition, the FY2021 William M. (Mac) Thornberry National Defense Authorization Act requires CISA to review the list of designated CI sectors and sector risk management agencies periodically and recommend appropriate changes to the President.[97]

The federal cybersecurity resources available to CI entities vary by sector, and in most cases, private CI operators are not required to use federal services or follow federal guidance.[98] There are several exceptions to this general rule. Notably, following the Colonial Pipeline attack, the Transportation Security Administration (TSA) issued a security directive in July 2021 requiring pipeline operators to "implement specific mitigation measures to protect against ransomware attacks and other known threats."[99]

One of CISA's primary CI-sector cybersecurity roles is to share information between public and private entities,[100] including vulnerability reports, threat assessments, and technical expertise. Like the laws governing CISA's federal preparedness mission, these laws likely encompass ransomware threats, requiring CISA to share threat assessments related to ransomware attacks.[101] To encourage private sector participation, Congress has authorized private entities to engage in network monitoring and defensive measures[102] and has shielded private entities from liability for both monitoring activity[103] and voluntary information sharing.[104]

---

[93] PPD-21, PRESIDENTIAL POLICY DIRECTIVE—CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013).

[94] *Id.*; *see Critical Infrastructure Sectors*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors (last visited Sept. 28, 2021).

[95] 6 U.S.C. §§ 651 (defining *sector risk management agency* as "a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with [DHS]"), 665d (outlining duties of sector risk management agencies).

[96] *See id.* §§ 652(c), 665d(c).

[97] *Id.* § 652a(b).

[98] *See* Dustin Volz, *Biden Directs Agencies to Develop Cybersecurity Standards for Critical Infrastructure*, WALL ST. J. (July 28, 2021), https://www.wsj.com/articles/biden-directs-agencies-to-develop-cybersecurity-standards-for-critical-infrastructure-11627477200.

[99] Press Release, U.S. Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (July 20, 2021), https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators. For more information on the Colonial Pipeline ransomware attack and pipeline security, see Parfomak & Jaikaran, *supra* note 6; CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran.

[100] 6 U.S.C. §§ 659 (establishing a "national cybersecurity and communications integration center"), 1503(c) (authorizing the sharing of cyber threat indicators with non-federal entities); *see Information Sharing and Awareness*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/information-sharing-and-awareness (last visited Sept. 28, 2021).

[101] *See Nat'l Cyber Awareness Sys. – Alerts*, *supra* note 87.

[102] 6 U.S.C. § 1503(b).

[103] *Id.* § 1505(a).

[104] *Id*. §§ 673, 1505(b). For more information on CI protection, see CRS Report R45809, *Critical Infrastructure:*

Data Protection and Privacy

In addition to the cyber preparedness laws described above, a number of federal data protection laws also impose cybersecurity requirements on private entities that collect a variety of information from consumers and other individuals. For example, the Gramm-Leach-Bliley Act,[105] which applies to financial institutions, directs financial regulatory agencies such as the Federal Trade Commission (FTC) to establish "Safeguards Rules."[106] The FTC has promulgated a regulation under the Act that requires covered institutions to implement "administrative, technical, and physical safeguards" to protect against, among other risks, unauthorized access to customer records.[107] Similarly, the Children's Online Privacy Protection Act (COPPA)[108] requires operators of websites or online services directed to children to protect the "confidentiality, security, and integrity" of any information collected from children.[109] Likewise, regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[110] require health care providers and certain others to "protect against any reasonably anticipated threats or hazards to the security or integrity" of electronic protected health information.[111]

Depending on the law at issue, a number of agencies, including the FTC, the Consumer Finance Protection Bureau, and the Department of Health and Human Services (HHS), enforce these data protection laws.[112] Although these laws largely predate the rise of ransomware, and so do not explicitly mention such attacks, at least one agency, HHS, has interpreted HIPAA's security rule to require protection against ransomware and other malware attacks.[113] It is likely that other data protection laws would similarly require covered entities to take steps to prevent ransomware attacks.

Emerging Trends and Policy Considerations for Congress, by Brian E. Humphreys.

[105] 15 U.S.C. ch. 94, subch. I.

[106] *Id.* § 6801(a) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."). A *financial institution* for purposes of the Gramm-Leach-Bliley Act is "any institution the business of which is engaging in financial activities as described in section 1543(k) of title 12," *U.S. Code*. *Id.* § 6809(3)(A).

[107] *Id.* § 6801(b) (requiring regulatory agencies to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards" to ensure data security and confidentiality); *see, e.g.*, 16 C.F.R. pt. 314 (2021) (Federal Trade Commission regulations implementing the "Safeguards Rule").

[108] 15 U.S.C. ch. 91.

[109] *Id.* § 6502(b)(1)(D).

[110] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[111] 45 C.F.R. § 164.306(a)(1). Entities covered by the HIPAA regulations include health plans, health care clearinghouses, and health care providers who transmit health information in electronic form. *Id.* § 160.102(a).

[112] *See, e.g.*, *Statutes Enforced or Administered by the Commission*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes (last visited Sept. 28, 2021); *Enforcement*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/enforcement/ (last visited Sept. 28, 2021); *HIPAA Enforcement*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 25, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html. For more information on these and other federal data protection laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[113] OFF. FOR CIV. RTS., U.S. DEP'T OF HEALTH & HUM. SVCS., FACT SHEET: RANSOMWARE AND HIPAA (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

Incident Response and Mitigation

When a cyber intrusion occurs, a number of federal laws may apply, depending on the target of the intrusion. For federal incidents—occurrences that jeopardize a federal information system or constitute "a violation of law, security policies, security procedures, or acceptable use policies"[114]—FISMA requires each agency to develop, document, and implement procedures for detecting, reporting, and responding to security incidents, including mitigating any risks "before substantial damage is done."[115] For *major incidents* (defined by OMB as incidents "likely to result in demonstrable harm" in an area such as national security or the economy[116]), FISMA requires agencies to notify Congress within seven days "after the date on which there is a reasonable basis to conclude that the major incident has occurred" and again within a reasonable time period with a more detailed summary of the incident.[117]

For private CI sector entities, there is no generally applicable law requiring disclosure of cyber intrusions, though at least two such bills have been introduced in the 117th Congress.[118] One of these bills—the Cyber Incident Reporting Act of 2021—would require covered entities to report ransom payments to CISA within twenty-four hours of a payment.[119] Some CI sectors, however, are subject to sector-specific reporting requirements; for example, the TSA issued a security directive in May 2021 obligating pipeline owners "to report confirmed and potential cybersecurity incidents" to CISA.[120]

Private entities that are not subject to mandatory disclosure rules may voluntarily report cyber incidents to either CISA or the FBI's Internet Crime Complaint Center.[121] Information submitted by a private CI sector entity for CI protection purposes is protected from disclosure and cannot be used in civil actions against the private entity.[122] Depending on the CI sector, however, sector-specific data protection laws may subject private entities to administrative penalties or civil liability if the entity failed to adequately safeguard protected information.[123]

Under Presidential Policy Directive 41, the federal government's response to cyber incidents, public or private, is guided by five principles: (1) shared responsibility; (2) risk-based responses; (3) respecting affected entities; (4) unity of governmental effort; and (5) enabling restoration and

[114] 44 U.S.C. § 3552(2).

[115] *Id.* § 3554(b)(7).

[116] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, M-18-02, FISCAL YEAR 2017-2018 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS 5 (2017).

[117] 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

[118] *See* Cyber Incident Notification Act of 2021, S. 2407, 117th Cong. (2021); Cyber Incident Reporting Act of 2021, S. 2875, 117th Cong. (2017).

[119] S. 2875, sec. 3(b), § 2232(a)(2).

[120] Press Release, U.S. Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[121] *See Report Incidents, Phishing, Malware, or Vulnerabilities*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://us-cert.cisa.gov/report (last visited Sept. 28, 2021); *Internet Crime Complaint Center IC3*, FED. BUREAU OF INVESTIGATION, https://www.ic3.gov (last visited Sept. 28, 2021).

[122] 6 U.S.C. § 673(a) (providing, in part, that voluntarily submitted critical infrastructure information shall not, without written consent, "be used . . . in any civil action arising under Federal or State law if such information is submitted in good faith").

[123] *See, e.g.*, 15 U.S.C. § 6805 (authorizing administrative enforcement of the Gramm-Leach-Bliley Act); 47 U.S.C. § 206 (allowing customers to sue for violations of the Communications Act of 1934, which includes several data privacy and security provisions).

recovery.[124] These principles require federal agencies to work together and with other entities, including state and local governments, to share information and respond to threats.[125] CISA again plays a coordinating role in this response; when a federal agency or private CI sector entity reports a cyber incident, CISA is required to provide crisis management support and technical assistance to federal agencies; state and local governments, as appropriate; and private CI sector entities, on request.[126] In addition, CISA is responsible for developing and maintaining the National Cyber Incident Response Plan, which specifies the roles that private entities, state and local governments, and federal agencies play in responding to cyber incidents.[127] Finally, the DHS Secretary can issue emergency directives to federal civilian agencies to help mitigate cyber incidents.[128]

Each of these authorities likely extends to ransomware attacks. In the event of a ransomware attack, affected federal agencies or CI sectors may be required to report the attacks to CISA, though some CI sectors may not have to do so under current law.[129] CISA is required to provide technical assistance to help federal agencies recover from ransomware attacks, and it may issue emergency directives, as appropriate.[130] For private CI entities, the sector risk management agencies may have the authority to issue binding directives, such as TSA's recent directives governing the pipeline sector.[131]

Author Information

Peter G. Berris
Legislative Attorney

Jonathan M. Gaffney
Legislative Attorney

[124] PPD-41, *supra* note 1.

[125] *Id.*

[126] 6 U.S.C. §§ 652(c), 655(1).

[127] *Id.* § 660(c); *see The National Cyber Incident Response Plan*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://us-cert.cisa.gov/ncirp (last visited Sept. 29, 2021).

[128] 44 U.S.C. § 3553(h)(1)(A); *see Cybersecurity Directives*, U.S. DEP'T OF HOMELAND SEC., https://cyber.dhs.gov/directives/ (last visited Sept. 29, 2021).

[129] *See* 44 U.S.C. § 3554(b)(7)(c)(ii) (requiring federal agencies to notify CISA of cyber incidents).

[130] 6 U.S.C. §§ 652(c), 655(1).

[131] *See supra* note 120.

Disclaimer