By Kyle W. Miller

New Rules, Regulations and Guidance Affect Reorganizations of Critical Infrastructure Entities

Kyle W. Miller
Dentons; Louisville, Ky.

Kyle Miller is a lawyer in Dentons's Global Data Privacy and Cybersecurity Group in Louisville, Ky. His practice builds on his previous career as a cybersecurity professional in bringing value to clients with needs related to cybersecurity, data privacy and technology.

Bankruptcy professionals have many obligations to protect the operations and data of their clients under state and federal laws, in addition to their professional duties and promises made in their contracts. In the past year, the federal government has added to the growing web of obligations for owners and operators of "critical infrastructure," including bankrupt organizations deemed critical infrastructure. As a threshold matter, organizations should understand whether they are considered critical infrastructure by the U.S. government. Unfortunately, a uniform definition or test has not been created.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (also referred to as the "USA Patriot Act") defines "critical infrastructure" 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."[1] In addition, the National Infrastructure Protection Plan (NIPP), published by the Department of Homeland Security in 2013, defines "critical infrastructure" as "assets, systems, and networks that underpin American society," while analyzing the impacts of risks at the national, regional and local levels.[2]

Historically, having a precise definition of "critical infrastructure" was not essential because the classifications were only used to establish voluntary public/private partnerships with the organizations that self-identified to the government. However, recent emphasis on critical infrastructure regulation will require stricter definitions. For now, the Cybersecurity and Infrastructure Security Agency (CISA) has jurisdiction over the following 16 defined critical infrastructure sectors along with a sector-specific agency in most instances:[3] chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

There have been efforts to officially register and proactively recognize organizations as critical infrastructure, including the National Critical Infrastructure Prioritization Program (NCIPP) and an interagency database of potentially critical organizations known as the Homeland Infrastructure Foundation-Level Data. However, there is no definitive system to determine whether an organization would be considered critical infrastructure. A 2022 Government Accountability Office report found that the NCIPP may be "of little use" and noted a "lack of use among critical infrastructure stakeholders."[4] Thus, an organization being represented might be deemed critical infrastructure without it having a current designation or registration. If a client is in one of the previously mentioned 16 sectors, you should understand the additional obligations that could be required.

Security Incident Notification

Organizations have historically only notified individuals or regulators about a cyberattack on its systems when compelled by law to do so. Thus, without a data breach notification statute mandating disclosure of the attack, many cyberattacks were only known to the professionals involved. Further adding to the secrecy, cybersecurity investigations are routinely performed by attorneys or on their behalf, and they attempt to shield the incidents using legal privilege. Recently, a slew of mandatory reporting rules and regulations have emerged to ensure that regulators and other stakeholders know about incidents soon after they occur. The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corp. published a joint final rule requiring banking organizations and their bank service providers to notify their regulators within 36 hours of determining that there was a "notification incident" disrupting operations.[5]

1 42 U.S.C. § 5195c(e).
2 "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Executive Summary," U.S. Dep't of Homeland Sec. (2013), p. 1.
3 Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, PPD-21.
4 "Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," U.S. Gov't Accountability Office, GAO-22-104279 (March 2022).
5 Final Rule, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 C.F.R. pt. 53; 12 C.F.R. pt. 225, 12 C.F.R. pt. 304.

In the wake of the Colonial Pipeline attack in May 2021, the Transportation Security Administration (TSA) enacted multiple Security Directives that require, among other things, reporting to the TSA within 24 hours of nearly any malicious activity affecting a network used by a pipeline owner/operator.[6] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) compels critical infrastructure organizations to be far more open about their cybersecurity posture and incidents. Once final CIRCIA rules are issued by the CISA, critical infrastructure organizations will have only 72 hours to notify the CISA once they "reasonably believe" that a reportable incident has occurred.[7] In addition, critical infrastructure organizations will have only 24 hours to notify the CISA after the organization pays a ransom to attackers.[8] Bankruptcy professionals should understand that representing critical infrastructure organizations will require more transparency, communication and obligatory reporting than they may otherwise be used to.

Cross-Sector Cybersecurity Performance Goals

In October 2022, the CISA released its Cross-Sector Cybersecurity Performance Goals (CPGs),[9] which are a prioritized subset of information technology and operational technology cybersecurity practices aimed at meaningfully reducing risks to business operations. The CPGs are "a minimum set of practices that organizations should implement and aim to help [critical infrastructure] entities ... the CPGs are intended to be a floor, not a ceiling, for what cybersecurity protections organizations should implement to reduce their cyber risk."[10]

Unlike other voluminous and detailed standards and frameworks, meeting the CPGs should be within reach for even small organizations with limited resources. The CISA specifically designed each CPG to (1) significantly reduce the risk of a common threat; (2) be clear, actionable and easily definable; and (3) be reasonably straightforward and not cost-prohibitive. For example, CPG 1.4 requires implementing multi-factor authentication. The costs of implementing multi-factor authentication organization-wide can vary with the number of accounts to authenticate and whether it is implemented with hardware or software, but each additional authentication factor drastically reduces the risk of a compromised account. Each CPG is similarly designed to have a significant reduction in risk once properly implemented.

While there is no current federal enforcement mechanism for the CPGs, private parties have begun to incorporate them in risk analyses. Critical-infrastructure organizations may soon find that their insurers are requiring them to conform to the CPGs in order to qualify for cybersecurity insurance and that credit-rating agencies have been asking for evidence of their meeting the CPGs in analyzing creditworthiness. Bankruptcy professionals should understand that meeting the minimum standards found in the CPGs may be essential to reaching a successful reorganization plan or achieving financing and acceptable interest rates. When asked, bankruptcy professionals may need to find resources in the organization that can answer detailed questions related to the CPGs.

CFIUS

In September 2022, President Joe Biden issued the first-ever Executive Order related to the Committee on Foreign Investment in the United States (CFIUS).[11] The Executive Order added cybersecurity considerations to CFIUS's ability to review transactions involving foreign investment of American companies, and it expressly states that CFIUS must ensure that foreign investment does not erode the nation's cybersecurity posture. In addition, it cautions that a foreign investor that can affect the operation of critical infrastructure may pose a risk to national security.[12] Ultimately, the Executive Order instructs CFIUS to consider "the cybersecurity posture, practices, capabilities, and access of both the foreign person and the United States business" in its review.[13] This review would require investigation into the cybersecurity capabilities of both the buyer and the seller.

Conclusion

Bankruptcy professionals recognize that foreign ownership may necessitate CFIUS review. However, the Executive Order clearly instructs CFIUS to review transactions related to cybersecurity and critical infrastructure. This expands CFIUS's scope and mandate while emphasizing the types of transactions about which the current administration is most concerned. More detailed reviews by CFIUS may slow down the restructuring process, especially if an organization's operations are considered critical to the security of the U.S., and the proposed new owners include foreign nationals and corporations. abi

6 TSA Security Directive Pipeline-2021-01A (2021); TSA Security Directive Pipeline-2021-01B (2022); TSA Security Directives Pipeline-2021-02C.
7 6 U.S.C. § 681b(a)(1).
8 6 U.S.C. § 681b(a)(2).
9 "Cross-Sector Cybersecurity Performance Goals," CISA (October 2022), *available at* cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf (last visited Feb. 22, 2023).
10 *Id.* at p. 5.
11 Executive Order 14083.
12 *Id.* at § 3.
13 *Id.*