TWCA Risk Management Fund

CYBER ALERT

March 22, 2022

Cyber Incident Reporting for Critical Infrastructure Act of 2022

On Tuesday March 15, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022. We received the following alert from Baker Botts. While we await the final rules to add clarity, we wanted to make you aware of these new cyber incident reporting requirements.

Reporting

Likely of greatest interest to most organizations is the mandatory reporting requirements; however, *which entities* and *which incidents* covered under the Act is still uncertain.

The Act defines a "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21." In turn, Presidential Policy Directive 21 identifies 16 critical infrastructure sectors that span a range of industries within the United States. Similarly, a "covered cyber incident" is "a substantial cyber incident experienced by a covered entity." Both "covered entities" and "covered incidents" are expected to be given final definitions in the rules to be developed by the Director of the Cybersecurity and Infrastructure Agency ("CISA" or "Agency"), as discussed below.

Notwithstanding these broad definitions, the actual reporting requirements are clearer and arise in two ways. First, a covered entity experiencing a covered cyber incident must report the incident to CISA within 72 hours after the covered entity reasonably believes the incident occurred. Second, in the event a covered entity makes *any* ransom payment (even if it is not in response to a covered incident), the entity must report the payment to CISA within 24 hours.

The exceptions to these reporting requirement are limited: (1) allowing a covered entity to make a single report to cover both a covered incident and a ransom payment; and (2) select reporting requirements to other Federal agencies will

satisfy the Act's reporting requirement provided that a sharing agreement between the agencies is in place.

The specific manner and form of reporting under the Act will be outlined in the Final Rules circulated by the Director, as described below.

Rulemaking

The Act sets forth specific provisions for the Director to establish rules and regulations for compliance with its requirements. These rules will be established through cooperation of the Director, Sector Risk Management Agencies, the Department of Justice, and other Federal agencies. Once prepared, the rules will be published in the Federal Register within **24 months** of enactment of the Act. Then, within **18 months** of publication in the Federal Register, the Final rules must be issued.

The Final Rules themselves are required to contain various information (which is otherwise not included specifically within the Act). The rules must include:

- Clear descriptions of "covered entities" based on a variety of elements, including consequences of disruption of their services, the risk that they will be attacked, and threat of information that could be extracted.
- Clear description of "covered cyber incidents," requiring at least a loss of integrity of a system, disruption of operations, or unauthorized access.
- Clear description of the content of a report under the Act, including a description of the event; a description of the exposed vulnerabilities; the identity of any known, or reasonably believed, threat actor; identification of categories of personal information affected; and the name of the affected covered entity, as well as contact information.
- The types of data that an organization is required to preserve in the event of an attack.
- The criteria for submitting supplemental reports for any covered incident.

Similar requirements must be provided for reports related to the payment of ransoms under the Act.

Enforcement

Beyond setting requirements for reporting, the Act also empowers CISA with enforcement powers, through subpoenas and civil enforcement suits against covered entities.

Generally, the Director must first request, if it has reason to suspect that a covered cyber incident has occurred, additional information from a covered entity for the purpose of confirming whether a covered incident or ransom payment has

occurred. The covered entity has **72 hours** to respond to the Director's request, after which time the Director may issue a subpoena to compel disclosure of information. If the covered entity fails to respond, the Director may refer the matter to the Attorney General to bring a civil action to enforce, and a court may sanction the organization for failure to comply with the subpoena with contempt of court.

Cooperation

To the extent allowed under Federal law, CISA may share any information that an organization provides under the Act (of either a covered cyber incident or a ransom payment) with any other Federal Agency *only for*:

- A cybersecurity purpose (which is not otherwise described or defined in the Act);
- Identifying a cyber threat or security vulnerability;
- Responding to specific threats of harm;
- Responding to a threat to a minor; or
- Responding to certain cyber incidents reported under the Cybersecurity Act of 2015.

When it receives any report, CISA is tasked with immediately determining if it relates to any ongoing threats or incidents and reporting the relevant information to the appropriate agency or body. But any sharing or cooperative ventures must protect personal information from unauthorized disclosure and use, including by those same agencies.

While CISA may share reported information, reporting entities may designate information as "commercial, financial and proprietary information" and receive certain protections. Furthermore, disclosure of such information does not serve as a waiver of any legal protections, including trade secrets, and is not subject to open records laws.

Conclusion

The Act also covers a variety of related new roles and responsibilities for CISA, including the creation of a "Cyber Incident Reporting Council," which is intended to increase cooperation and responsiveness of Federal agencies to cyber-attacks against critical infrastructure.

*The Sectors are: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food & Agriculture, Government Facilities, Healthcare & Public Health, Information Technology, Nuclear Reactors, Materials & Waste, Transportation Systems, and Water & Wastewater Systems.