Freshfields Bruckhaus Deringer

U.S. Government Levies New Cyber Incident Report Requirements on Private Sector

Authored by: Brock Dahl
March 22, 2022

The President recently signed the 2022 Consolidated Appropriations Act that included, nestled within its thousand pages, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the Act). The Act will fundamentally alter the cyber reporting relationship between relevant segments of the private sector and the federal government, primarily the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Amongst other things, the Act levies mandatory reporting requirements on a community of corporate entities (to be defined in regulation) for a variety of incidents (to be defined in regulation) and ransom payments made in response during such incidents.

Mandatory Reporting of Cyber Incidents and Ransom Payments. The Act creates:

- a 72-hour report requirement for cyber incidents suffered by covered entities. The three-day window is initiated when the entity "reasonably believes that the covered cyber incident has occurred;" and,
- a 24-hour reporting requirement when a covered entity has made a ransom payment.

Covered Entities - to be Defined. The Act leaves it to CISA to define what entities are within the reporting scope. The Act does focus on entities within any of the sixteen critical infrastructure sectors previously defined through Presidential directive, leaving only a limited swath of the U.S. economy possibly outside its ambit. Not later than March 15, 2024, CISA must issue a notice of proposed rulemaking to further define entities qualifying as covered entities. Judging by CISA Director Jen Easterly's enthusiasm for the Act, DHS will not take nearly so long to issue the proposal. Once issued, CISA will then have no more than 18 months to issue a final rule.

Covered Cyber Incidents - to be Defined. The Act also defers to the same CISA regulatory action as mentioned above for further description of the scope of covered cyber incidents. It does provide some guidance to CISA, and specifically excludes from the scope of the requirement imminent threats that have not yet materialized. More specifically, it outlines a few categories of events that it requires to be included in the final rule. Those include cyber incidents:

- yielding a "substantial loss" of confidentiality, integrity, or availability of certain information systems and networks, or a "serious impact" on safety and resiliency of operational systems and processes. The distinction between information and operational systems speaks to a traditional dividing line in critical infrastructure between systems that can loosely be defined as business systems (information) versus industrial control systems (operational)

that are used to govern infrastructure functions (turning on and off, throttling flows, etc.). Those categories admittedly require further interpretation of subjective terms, such as "substantial loss" and "serious impact," but their application to distinct systems will provide some grounds for more definitive interpretations of reporting triggers.

- causing a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero-day vulnerability, against both information and operational systems. Here, a mere "disruption" could encompass a wide range of events, and it will be helpful for CISA's proposed rule to clarify what is meant by this term.

- unauthorized access or "disruption" of operations caused by impairments to service providers.

Congress also orders CISA to consider a variety of factors in establishing the scope of covered incidents, including the sophistication or novelty of the attack, the number of individuals affected, and the potential impacts on industrial control systems.

Needless to say, the proposed rulemaking will be critical to shedding more light on the direction and scope of these requirements and providing an opportunity for feedback before the rule is finalized.

Supplemental Updates. The statute also requires covered entities to file supplemental reports "if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting an initial report." This obligation persists until the time that the entity notifies CISA that the issue has been fully mitigated and resolved. Like some of the more ambiguous terms above, this will yield questions about what type of information is considered "substantial," but the final rule issued by DHS is also supposed to "provide a clear description" of what constitutes such information.

Liability and Information Protections. Similar to the Cybersecurity Information Sharing Act of 2015, a statute that sought to encourage voluntary private sector reporting of the nature now being made mandatory, the Act provides several protections for corporate reporters that properly submit their information.

Enforcement Protections. Federal, State, Local, or Tribal governments shall not use information about a covered cyber incident or ransom payment submitted through direct reporting to regulate or pursue an enforcement action "unless the government entity expressly allows entities to submit reports" to CISA to meet regulatory reporting obligations. That is a strange caveat that will have to be amplified, but is unlikely to be significant in practice since most regulators will not be likely to cede direct reporting rights to another agency.

- Disclosure Protections. Companies may mark their submissions as proprietary information, and properly submitted information will ostensibly be protected from FOIA requests. The

submission will also not be considered to constitute a waiver of any applicable privileges and protections provided by law.

- Liability Protections. The Act states that no party can bring a cause of action on the basis of the fact of the submission, but note that this exclusion applies to the fact of the submission only, not necessarily its substance. Moreover, the Act also states that submitted reports, or communications or materials crated in preparing the report, may not be received in evidence or otherwise subject to discovery in a federal or state court or regulatory body.

Punitive Abilities. CISA will retain the ability to issue subpoenas where the Director determines a company should be submitting a report, but has not done so. The Director can then refer matters for civil enforcement to the Attorney General where an entity has not complied with the subpoena, and a court may punish such failure to comply with the subpoena as contempt of court.

Notwithstanding the protections provided above, one clause that is likely to draw significant attention is the ability of the CISA Director, where information is acquired pursuant to a subpoena, to provide information to the Attorney General, or the head of the "appropriate Federal regulatory agency," where the Director feels the "facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution[.]" That same power does not appear to exist where companies have proactively provided the information, rather than doing so subject to subpoena.

Conclusion. For the time being, potentially affected entities should keep a close eye on the notice of proposed rulemaking and be prepared to provide feedback on points of ambiguity. In particular, there will be further interest in refining categories of ambiguous terms relating to reporting triggers, such as "substantial loss," "serious impact," and "disruption." Parties that feel it is likely that they may fall within the requirements may also wish to consider the current readiness of their internal incident compliance and reporting architecture, as the period for incurring obligations under the statute is unlikely to be delayed for too long.