Published on *The National Law Review* https://natlawreview.com

Top Five Takeaways for Businesses from the New CISA Cyber Reporting Act

Article By:

Kristin L. Bryan

Ericka A. Johnson

James Brennan

As covered here at CPW, President Biden recently signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Act"). While the Act presents a plethora of issues for litigators and compliance professionals to consider, CPW has identified five key points that businesses should know about the Act:

1. **Many Critical Ambiguities Are Left to CISA Rulemaking, and the Act Is not Effective Until CISA's Final Rule**

Key terms in the Act—including (*i*) which "**covered entities**" must report cyber incident and ransom payments to the Cybersecurity and Infrastructure Security Agency ("CISA"), (*ii*) which cyber incidents are "**covered cyber incidents**" triggering the reporting requirement, and (*iii*) which data must be preserved as "**relevant**" to a cyber incident or ransom payment—are explicitly left for CISA to define through rulemaking. *See* new § 2242(c)(1)–(2), (6). The Act establishes two deadlines for CISA's rulemaking: CISA has 24 months after enactment to issue a proposed rule, and CISA has 18 months after the proposed rule to issue the final rule. § 2242(b). However, the Act does not provide a minimum amount of time before CISA issues either the proposed or final rule, so some clarity on critical definitions may come much sooner. The final rule will be key not only for its clarification of key terms, but because the effective date of the Act's reporting requirements will be prescribed in the final rule. § 2242(a)(7).

2. **The 72-Hour Clock for Cyber Incident Reporting Starts with "Reasonable Belief"**

The Act requires that "[a] covered entity that experiences a covered cyber incident shall report the covered cyber incident to [CISA] ***not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred***." § 2242(a)(1)(A). There is no statutory definition of "reasonably believes," and it is unclear whether the term will be interpreted by CISA's

final rule or left to be determined through enforcement and litigation. Any future guidance will prove valuable, as there are many hypothetical scenarios where an entity's reporting obligations may turn on the meaning of "reasonably believes . . . ." For example, if one employee of an entity believes a covered cyber incident occurred but does not report it to an officer until the next day, which person's belief starts the timer? If a covered entity knows that a "cyber incident" has occurred, but determines with the best information available that the cyber incident does not rise to the level a "covered cyber incident," is that belief protected as "reasonable" if later information shows the incident would in fact be a "covered" cyber incident? CPW will keep you in the loop when any similar legislation offers clues to how this provision will be interpreted.

3. Ransom Payment Reports Are Required Even in the Absence of a Covered Cyber Incident

In addition to the cover cyber incident reporting requirement, the Act requires that "[a] covered entity ***that makes a ransom payment as the result of a ransomware attack*** against the covered entity shall report the payment to [CISA] ***not later than 24 hours after the ransom payment has been made***." § 2242(a)(2)(A). A "ransomware attack" is defined directly in the Act to include extortion via "the use or threat of use of unauthorized or malicious code on an information system" or other digital mechanism to disrupt the system or comprise its data. § 2240(14). The Act makes clear that a ransom payment report is required whenever a ransom payment is made in connection with a ransomware attack, even if the ransomware attack does not fall within the definition of a "covered cyber incident." § 2242(a)(2)(B). If the ransomware attack ***is also*** a covered cyber incident, it is possible for an entity to file one report covering both reporting requirements. § 2242(a)(5).

4. Complying with the Reporting Requirements Will Have Benefits, and Non-Compliance Will Have Costs

The required contents of covered cyber incident and ransom payment reports, as well as the procedures to file them, will be fleshed out in the CISA final rule. § 2242(c)(4)–(5), (7)–(9). But the Act directly establishes incentives for compliance and possible consequences for non-compliance.

Reports in compliance with CISA are afforded certain confidentiality and liability protections. With respect to confidentiality, the Act provides that reports submitted to CISA shall be considered the proprietary information of the covered entity if so designated by the covered entity. § 2245(b)(1). Furthermore, the submission of a report ***is not*** considered a waiver of any privilege or trade secret protection, § 2245(b)(3), and the reports are exempt from disclosure under the Freedom of Information Act and similar state and local laws, § 2245(b)(2). As to liability, the Act eliminates any cause of action based "solely" on the proper submission of a covered cyber incident report or ransom payment report to CISA. § 2245(c). The Act also expressly prohibits federal, state, and local agencies from engaging in regulatory enforcement on the basis of information obtained "solely" through reports submitted to CISA. § 2245(a)(5).

If an entity does ***not*** comply with the reporting requirements, CISA's enforcement proceeds in two stages. § 2244(a). ***First***, CISA may make an initial request for information from an entity about a covered cyber incident or ransom payment. § 2244(b)(1). If the entity discloses information at this stage, then the information will be deemed as coming through a proper report and receive all the confidentiality and liability protections discussed above. § 2244(b)(2).

Second, if a covered entity does not respond to such initial request for information within 72 hours (or responds inadequately), CISA may issue a subpoena compelling the disclosure of information that was required to be reported. § 2244(c)(1). CISA may also bring a civil action in federal district court to compel compliance with the subpoena, § 2244(c)(2), and provide information to other federal agencies for possible regulatory enforcement or prosecution, § 2244(d). Significantly, the confidentiality and liability guarantees described above ***do not apply*** to information that is disclosed to CISA pursuant to a subpoena.

In fact, the Act explicitly provides that based upon the information provided in the subpoena, the "Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution." § 2244(d).

5. **Other Federal Reporting Obligations May Obviate CISA Reporting, but not Immediately**

The Act provides an exemption to reporting requirements when the covered entity is "required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe." § 2242(a)(5)(b)(i). Putting aside the meaning of "substantially similar"—which will also be defined by the final rule—this exemption will only become effective after CISA has entered into an interagency agreement with the other federal agency that receives the substantially similar report. § 2245(a)(5)(b)(ii). This means that an entity which is already required to file a substantially similar cyber incident report with another federal agency will have to comply with duplicative reporting schemes until an interagency agreement is reached.[1] Still, because of the potential for a covered entity to effectively satisfy the Act's reporting requirement via another federal reporting scheme, covered entities have an additional incentive today to ensure compliance with existing federal reporting requirements.

FOOTNOTES

[1] If a covered entity reports to CISA (in lieu of its obligation to report to another Federal agency via an interagency agreement) the reporting protections do not exist. *See* 2245(a)(5)(A).

National Law Review, Volume XII, Number 84