

President Biden Signs into Law the Cyber Incident and Reporting Act, Mandating Reporting of Cyber Incidents and Ransomware Payments

Article By:

Brian G. Cesaratto

Allen R. Killworth

On March 15, 2022, President Biden signed into law the [2022 Consolidated Appropriations Act](#) containing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the “Cyber Incident Reporting Act”). While President Biden’s remarks highlighted the [\\$13.6 billion in funding](#) “to address Russia’s invasion of Ukraine and the impact on surrounding countries,” the 2022 Consolidated Appropriations Act contained numerous other laws, including the Cyber Incident Reporting Act, which should not be overlooked. The Cyber Incident Reporting Act puts in motion important new cybersecurity reporting requirements that will likely apply to businesses in almost every major sector of the economy, including health care, financial services, energy, transportation and commercial facilities. Critical infrastructure entities should monitor the upcoming rule-making by the Cybersecurity and Infrastructure Security Agency (“CISA”), as the final regulations will clarify the scope and application of the new law.

Reporting Requirements

The Cyber Incident Reporting Act imposes four primary reporting and related requirements on “covered entities” in the event of a “covered cyber incident” or a ransomware payment. Covered entities are defined by reference to [Presidential Policy Directive 21](#), setting forth 16 critical infrastructure industries.

First, a covered entity that experiences a “covered cyber incident” must report that incident to CISA no later than 72 hours after the covered entity reasonably believes that the covered cyber incident occurred. A “covered cyber incident” means an “occurrence” that actually “jeopardizes, without lawful authority, the integrity, confidentiality, or availability of” information on an information system or that information system, which is “substantial” and satisfies criteria to be established through future rule-making. The meaning of “substantial” will be subject to future rule-making by CISA, as will the precise contents of what must be disclosed in such a report, although the law provides that the following shall be included:

-
- Identification and a description of the function of the affected information systems, networks that were, or are reasonably believed to have been affected by such cyber incident;
 - A description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information systems or network or disruption of business or industrial operations;
 - The estimated date range of such incident; and
 - The impact to the operations of the covered entity.^[1]

Second, a covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity must report the payment to CISA not later than 24 hours after the ransom payment has been made. A “ransomware attack” is defined as an incident that includes “the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for ransom payment.”^[2] Notably, this shorter 24 hour reporting requirement applies even if the ransomware attack does not meet the definition of a “covered cyber incident.” CISA will provide clarity as to the contents of such a report in subsequent rulemaking.

Third, a covered entity must “promptly” submit to CISA an update or supplement to a previously submitted covered cyber incident report if “substantial new or different information becomes available” or if the covered entity makes a ransom payment after submitting a covered cyber incident report. This ongoing supplemental reporting requirement remains in effect until the covered entity notifies CISA that the incident has concluded.

Fourth, a covered entity must preserve data relevant to the covered cyber incident or ransom payment.

Covered Entities and Application to the Health Care and Other Industries

The Cyber Incident Reporting Act calls for CISA to define “covered entity” in future rulemaking from among entities in a critical infrastructure sector, as defined in Presidential Policy Directive 21. Presidential Policy Directive 21 identifies sixteen critical infrastructure sectors, including “Healthcare and “Public Health” as well as sectors covering broad segments of business such as “Commercial Facilities,” “Communications,” “Financial Services,” “Critical Manufacturing,” “Energy,” “Information Technology,” and “Transportation Systems” among others.

As “Healthcare and Public Health” is an identified critical infrastructure sector, health care entities should anticipate being subject to the Cyber Incident Reporting Act as “covered entities” (which is not identical to the term as defined under the Health Insurance Portability and Accountability Act (“HIPAA”)). The Cyber Incident Reporting Act contains an exception to the reporting requirement for covered entities “required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe” and provided that the Federal agency receiving such reports has an agreement in place to share such information with CISA. As HIPAA does not require reporting of covered cybersecurity incidents or ransomware payments as defined under the Act to any Federal agency, HIPAA covered entities are not excepted from the

reporting requirements of the Cyber Incident Reporting Act at this time.

It should be noted also that the definition of “cyber incident” does not require that protected health information be involved in the incident. Thus, a HIPAA covered entity could suffer a reportable cyber incident that is not a “breach” or “security incident” under HIPAA. In addition, the Cyber Incident Reporting Act has short 24 or 72 hour windows for reporting, in comparison to the longer time periods for reporting a breach of protected health information prescribed by the HIPAA breach notification rule.

Similarly, while we await the final rulemaking, further clarification and potential agency sharing agreements, other critical infrastructure entities should anticipate being subject to the reporting and data preservation requirements. This rule will significantly broaden existing breach reporting and incident response requirements for many organizations, and goes well beyond breach notification laws that are limited by data type as the reporting requirements extend here to all information and information systems held by the covered entity. The Act also expressly recognizes that businesses may need assistance of third party cybersecurity expertise in fulfilling their obligations, including providing that law firms and incident responders may submit the reports on their behalf.

Effective Date

The reporting requirements of the Cyber Incident Report Act will not go into effect until the final rules are promulgated under the Act. Presently, the law directs CISA, together with the Department of Justice and other federal agencies, to publish a notice of proposed rule-making within 24 months of the date of the enactment of the law, and that a final rule should be issued by CISA no later than 18 months after publication of the proposed rule-making.

ENDNOTES

[1] Sec. 2242(b)(4).

[2] Sec. 2240(d)

©2025 Epstein Becker & Green, P.C. All rights reserved.

National Law Review, Volume XII, Number 78

Source URL: <https://natlawreview.com/article/president-biden-signs-law-cyber-incident-and-reporting-act-mandating-reporting-cyber>