CONGRESS PASSES BROAD LEGISLATION REQUIRING CRITICAL INFRASTRUCTURE SECTORS TO REPORT SUBSTANTIAL CYBER INCIDENTS AND RANSOMWARE PAYMENTS

On March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Act") as part of the Consolidated Appropriations Act of 2022. The Act requires critical infrastructure providers to report substantial cyber incidents within 72 hours, report ransomware attack payments within 24 hours, and submit periodic updates on ongoing cyber incidents. This statute is the first federal law to require reporting of cyber incidents across a wide range of industries. These requirements will take effect upon the finalization of implementing regulations by the Cybersecurity and Infrastructure Security Agency ("CISA").

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 marks a major milestone in the US government's ongoing efforts to expand cybersecurity disclosure. Congress has previously encouraged cyber incident reporting when it passed the Cybersecurity Information Sharing Act of 2015, which provides limited legal protection for companies that share information on cyber attacks with the government or among themselves. But such reports were not mandatory. Now, following heightened concern regarding cyber attacks after Russia's invasion of Ukraine, Congress has taken more aggressive action.

REPORTING REQUIREMENTS

The Act requires "covered entities" to report to CISA "covered cyber incidents" and payments made in response to a ransomware attack.

Who is considered a "covered entity"?

The definition of "covered entity" will be refined by CISA rulemaking. However, at a minimum, the Act requires "covered entities" to include companies within the critical infrastructure sector, as defined by Presidential Policy Directive 21. This Directive broadly defines the critical infrastructure sector to include 16 industries

Attorney Advertising: Prior results do not guarantee a similar outcome

encompassing a large portion of the private sector, including the financial services, communications, healthcare, critical manufacturing, and food and agriculture industries.

What events must be reported?

Covered entities only need to report "substantial" cyber incidents. However, the Act leaves it to CISA to define what types of substantial incidents would be "covered cyber incidents." At a minimum, a "covered cyber incident" must include the occurrence of:

- substantial loss of confidentiality, integrity, or availability of an information system or network;
- disruption of business or industry operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero-day vulnerability; or
- unauthorized access or disruption of business or industrial operations due to loss of service caused by a compromised cloud service provider, managed service provider, or other third-party data hosting provider.

Additionally, in determining what types of cyber incidents must be reported the Act requires CISA to consider the sophistication or novelty of tactics utilized, the volume and sensitivity of the data at issue, the number of individuals affected, as well as any potential impact on industrial control systems.

The Act also separately requires covered entities to report ransomware payments.

What is the deadline for reporting?

Covered entities are required to report covered cyber incidents within 72 hours after the entity reasonably believes the incident has occurred and must report ransomware payments within 24 hours of making a payment.

Am I required to update reports?

The Act requires covered entities to promptly update CISA as new or different information about a previously reported incident is discovered. Covered entities must continue providing updates until they can inform the agency that the incident has been fully resolved.

Additionally, covered entities must update CISA if they make a ransom payment after submitting a covered cyber incident report.

What information must be included in a report?

Though more specific guidance will be provided through rulemaking, the Act sets out the baseline requirements for information that must be included in reports. This includes:

- a description of the incident, including details on which systems or devices were affected, the nature of any unauthorized access, and the date range and impact of the incident on the entity;

- a description of the vulnerabilities exploited and security defences the entity had in place at the time of the incident, as well as the tactics used to perpetrate the incident;
- any identifying or contact information about the attacker reasonably believed to be responsible for the incident;
- identification of the categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person;
- the name and contact information of the covered entity impacted by the incident.

Covered entities should provide the following information in ransomware payment reports:

- a description of the ransomware attack, including the estimated date range of the ransomware attack;
- a description of the vulnerabilities, tactics, and procedures used to perpetrate the ransomware attack;
- any identifying or contact information about the actor reasonably believed to be responsible for the ransomware attack;
- name and contact information of the covered entity that paid the ransom, or on whose behalf the ransom was paid;
- specific details regarding the ransom payment, including the date payment was made, the type of payment requested (e.g., cryptocurrency), payment instructions, and the amount.

The Act also requires entities to preserve data relevant to covered cyber incidents and ransomware payments in accordance with procedures that will be described in the final rules.

Are reports public?

Unlike some disclosures required under other regulations, such as the SEC's proposed cybersecurity rules for public companies, reports made pursuant to the Act will not be public.[1] If CISA shares any information from reports with entities other than federal agencies, it must anonymize the data. The Act also requires CISA to implement procedures for protecting individuals' privacy rights by anonymizing, safeguarding, or deleting personal information from reports that is not directly related to a cybersecurity threat.

Additionally, the Act exempts reports from disclosure under the Freedom of Information Act and similar laws. Further, the Act provides that by making a report a covered entity does not waive any applicable legal privilege or protection, including trade secret protection. The Act also prevents reports from being used as the basis for an enforcement action (except for litigation to enforce a CISA

1 For more on the SEC's recently proposed cybersecurity rules for public companies, see our briefing here: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/03/SEC%20Proposes%20Expansive%20New%20Cybersecurity%20Disclosure%20Regulations%20For%20Public%20Companies.pdf

subpoena, discussed further below) or received in evidence or otherwise used in any trial, hearing, or other proceeding.

What if I am already required to report similar incidents under other regulations?

In drafting the Act, Congress recognized that some critical infrastructure providers may already be subject to other cyber incident reporting regulations. To address this, the Act creates an exception whereby a covered entity will not have to file a report with CISA if it must file a substantially similar report with another federal agency. Importantly, however, this exception applies only if CISA has an information-sharing mechanism in place with the relevant federal agency. The exception also does not apply to state agencies.

The Act also requires CISA to consider existing regulatory reporting requirements and make efforts to harmonize these reporting obligations to the extent possible.

ENFORCEMENT

Notably, the Act gives CISA new enforcement powers to ensure covered entities comply with this law. CISA is authorized to request information from a covered entity that it believes was required to submit a cyber incident or ransomware payment report and failed to do so. If CISA does not receive a response or receives an inadequate response within 72 hours from requesting such information, it may issue a subpoena to the entity to compel disclosure of any information the agency deems necessary to determine whether a covered cyber incident or ransomware payment has occurred and any other information required to be reported.

If a covered entity does not comply with a subpoena, the Department of Justice may bring a civil action to enforce the subpoena. Additionally, if CISA determines that information obtained via a subpoena may constitute grounds for regulatory enforcement action or criminal prosecution, it may provide such information to the Department of Justice or to the relevant federal regulatory agency, who may then use that information to pursue an enforcement action against the entity.

TAKEAWAYS

As CISA Director Jen Easterly noted in her public remarks upon the Act's passing, this legislation is a "game-changer" for the federal government that will give CISA the data and authority to better protect US critical infrastructure providers from cyber attacks. However, the Act also imposes substantial new regulatory burdens on many companies.

The Act's requirements are not immediately effective. CISA has up to 24 months to issue a notice of proposed rulemaking, followed by 18 months to publish a final rule. Only then will these requirements take effect.

Critical infrastructure providers can begin taking steps now to ensure future compliance. Once enacted, the 72-hour and 24-hour reporting windows will require entities to be vigilant in early cyber incident detection and ensure a streamlined internal escalation process is in place. Critical infrastructure providers should also select and engage key service providers before an incident occurs.

Lastly, companies should consider how these new reporting requirements will impact existing reporting obligations under both state and federal laws. By taking stock of all applicable regulatory reporting obligations, critical infrastructure providers can ensure they are ready to expeditiously report incidents to the necessary agencies when incidents arise.

Clifford Chance has published a number of reports to help companies protect themselves from cyber attacks and comply with international reporting requirements. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Shannon O'Brien
Law Clerk

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2022

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.