ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

MARCH 17, 2022

New Cybersecurity Law Will Require Cyber-Incident Reporting for Critical Infrastructure

by *Kim Peretti*, *Kellen Dwyer*, and **Kristen Bartolotta**

On March 1, the Senate unanimously passed the Strengthening American Cybersecurity Act of 2022, which will require critical infrastructure companies to report significant cyber-incidents and all ransom payments to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The Act was included in the 2022 omnibus spending bill, which President Biden signed into law on March 15. Here is what companies need to know.

Which companies will be covered?

The Act delegates to CISA the power to define which entities will be subject to the Act's reporting obligations but contemplates that CISA will use its rulemaking power to cover entities that own and operate the nation's critical infrastructure. Indeed, the portion of the Act that contains the reporting mandates is titled the "Cyber Incident Reporting for Critical Infrastructure Act of 2022." The Act also provides that CISA shall define "covered entities" under the Act "based on (A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure." CISA is likely to define "covered entities" broadly to ensure that it receives reporting from a variety of sectors. At a minimum, CISA will likely define "covered entities" to encompass the 16 sectors currently considered "critical infrastructure" under Presidential Policy Directive 21:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing

- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

It is possible that CISA will go further and designate additional sectors as covered entities under the Act.

What types of covered cyber-incidents must be reported?

The definition of a "covered cyber-incident" will also be determined by CISA rulemaking. But the Act provides, at a minimum, that an incident must be reported if it: (1) causes a "substantial loss of confidentiality, integrity, or availability" of information or a "serious impact on the safety and resiliency of operational systems and processes"; (2) causes a "disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability"; or (3) involves "unauthorized access or disruption of business or industrial operations" due to a "compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." The last category is a clear reference to the recent SolarWinds and Microsoft Exchange hacks, which demonstrated that a threat actor can compromise one commonly used service or product and use that access to compromise hundreds or thousands of entities that use the product or service.

What types of ransom payments are covered?

Any payment to a threat actor made to avoid actual or threatened loss of confidentiality, availability, or integrity of data is considered a covered ransom payment. Indeed, the Act defines "ransomware attack" broadly to include more than the traditional ransomware attack involving the encryption of data. The definition also includes the use, or threatened use, of unauthorized malicious code, denial of service attacks, and any other mechanism designed to disrupt the operations of any entity's information system. Companies should note that this definition includes extortion events that occur without the use of ransomware.

When must cyber-incidents and ransom payments be reported?

The Act requires covered entities to report covered cyber-incidents within 72 hours after the entity "reasonably believes" such an incident has occurred. Ransom payments must be reported within 24 hours of payment. The Act does not specify exactly what it means for a company to have a reasonable belief that a covered cyber-incident occurred, but the reasonable belief requirement appears to be borrowed from state data breach notification laws. Companies should be aware that the reasonable belief standard could require reporting even if a breach has not in

fact occurred. In addition, the Act does not state whose reasonable belief triggers the 72-hour reporting requirement. Companies should consider addressing these questions in their security incident response plans.

What information must be reported?

Though the specifics are also subject to subsequent rulemaking by CISA, the Act establishes certain minimum reporting requirements. The contents of a cyber-incident report shall include, if "applicable and available":

- A description of the covered incident.
- A description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber-incident.
- Any identifying or contact information related to each actor reasonably believed to be responsible for the cyber-incident.
- The category or categories of information that were, or are reasonably believed to have been, subject to unauthorized access or acquisition.
- Information about the impacted entity, including state of incorporation or formation, legal entity name, trade names, or other identifiers.
- Contact information for the covered entity or an authorized agent of the entity.

Covered entities would be required to supplement initial reporting whenever substantial new or different information becomes available. Subsequent reporting would be required until the entity notifies CISA that the cyber-incident has been resolved. If a covered entity is required by law, regulation, or contract to report substantially similar information to another federal agency within a similar timeframe, then that entity may be excepted from reporting obligations established in the Act.

Reporting of ransom payments will include, at a minimum, if available and applicable:

- A description of the attack, including estimated date range of the attack.
- A description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.
- Any identifying or contact information related to each actor reasonably believed to be responsible for the ransomware attack.
- The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.
- Contact information for the covered entity or an authorized agent of the entity.
- The date of the ransom payment.
- The ransom payment demand, including the type of virtual currency or other commodity requested.
- The ransom payment instructions.
- The amount of the ransom payment.

Reporting of ransom payments would be required even if the ransomware attack is not a covered cyber-incident under the law.

Content requirements for reporting of both covered cyber-incidents and ransom payments are more expansive under the Act than in existing reporting requirements under state and federal law. While companies are likely used to providing information to law enforcement to help catch criminals, the focus of the Act is on providing CISA the information it needs to assess cyber-risk and update industry on emerging threats. This means that companies will be required to provide more sensitive information, including what specific vulnerabilities were exploited and security defenses were in place.

Who would receive the reports required by the Act?

CISA. Companies are not required to report directly to the FBI, which is reportedly among the reasons why the Justice Department has publicly opposed the Act. The Act does provide, however, for a mechanism for CISA to share information with other agencies. Within 24 hours of receiving a covered cyber-incident or ransom payment report, or information voluntarily submitted about a non-covered cyber-incident, CISA shall "make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies." Presumably, the FBI will be among the appropriate federal agencies that will receive such reporting from CISA. Additionally, CISA may share information from the reports with state regulatory agencies, as well as private entities such as technology and cybersecurity companies, but is required to do so in an anonymized fashion.

Will the information companies provide to CISA be used against them?

Not directly, but companies still need to be careful. The Act provides that no cause of action can be brought or maintained in court based "solely" on "the submission of a report" required by this Act. Nor can information "obtained solely through reporting directly" to CISA be used by any governmental entity to regulate the reporting entity or bring an enforcement action against the reporting entity. The Act further provides that submitting reports to CISA shall not be considered a waiver of privilege, nor shall the reports be subject to Freedom of Information Act requests. Finally, the Act creates a privilege, shielding the CISA reports from discovery or use in any litigation (state or federal), as well as "any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report."

While these are robust protections that should give companies some solace, companies should note that the word "solely" is repeatedly used. Thus, while regulators cannot use CISA reports themselves against companies, regulators are free to use the reports as leads to investigate companies and ultimately bring enforcement actions. Similarly, it will surely be hotly contested in civil data breach litigation exactly which documents or communications were created solely for CISA reporting, and are thus protected from discovery, and which would have been created regardless of the reporting requirements of the Act.

What are the penalties for noncompliance?

The Act does not appear to provide for penalties for failure to report within the specified time limits or for submitting inadequate reports, at least not in the first instance. The Act does provide that CISA may request information from a company to confirm whether a covered cyber-incident or ransom payment has occurred. If a company does not respond to CISA's information request within 72 hours, CISA may follow up with a subpoena. If the company does not comply with the subpoena, CISA may refer the matter to the Justice Department, which may bring an action to enforce the subpoena and, if necessary, hold a noncomplying company in contempt.

How can companies influence CISA's implementing rules?

Companies should take advantage of the notice-and-comment process of rulemaking, which builds in time for receipt and consideration of public comment. CISA has two years to publish a notice of proposed rulemaking in the *Federal Register*; that proposed rule will include a call for comments. Before the release of the proposed rule, it is possible that CISA may publish an advance notice of proposed rulemaking and accept public comments to get more information on the issue. However, companies will generally submit comments on the proposed rule during the specified comment period. Comment periods tend to range from 30 to 60 days, but the period can vary. Companies interested in submitting a comment to CISA's proposed rule should reach out to one of the attorneys listed below or to the Alston & Bird attorney with whom they maintain a relationship.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**:

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Kellen Dwyer
202.239.3240
212.905.9340
kellen.dwyer@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

ALSTON & BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

WWW.ALSTON.COM