March 22, 2022

New Critical Infrastructure Cybersecurity Implementing New Breach Notification Requirements Signed into Law

Client Bulletins

Authors: **Ryan T. Sulkin**, **Luke Schaetzel**

The new law will require critical infrastructure entities to report certain covered cybersecurity incidents to government agencies within 72 hours; ransomware payments within 24 hours.

On March 15, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law as a part of the federal government's omnibus appropriations bill to fund the government through the 2022 fiscal year. The new law's requirements will take effect pursuant to the timeframe laid out in the yet to be drafted or published regulations.

Under the new critical infrastructure law entities are required to report certain cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency ("**CISA**") within 72 hours and to report ransomware payments to CISA within 24 hours.

The full scope of the law will be determined by rulemaking and forthcoming CISA regulations. Currently, the only clarify as to scope is that the requirements might apply to entities that operate in certain sectors (as discussed below). It is not otherwise clear what specific attributes or characteristics will bring an entity into the law's scope and what sorts of cybersecurity incidents would trigger the notification requirements. The applicable rules and regulations will be proposed no later than within 24 months.

The new law passed Congress at a time when the federal government is continuously adding new tools to its repertoire in a battle against the exponential increase in hacks, data breaches, and ransomware attacks that have targeted both the public and private sector. A number of recent cybersecurity incidents targeted government agencies such as NASA and the FAA. For example, it is estimated that defense industry contractors and the Department of Defense lose almost $600 million annually as a result of cybersecurity incidents. Another example is the high profile SolarWinds hack that resulted in the largest breach of U.S. government information in recent years.

Additionally, cybersecurity attacks on private entities that have far reaching, national impacts have increased as well. For example, a ransomware attack on a Colonial Pipeline Company system in 2021caused gas shortages across the southern and eastern regions of the U.S.

The new critical infrastructure law is one of many recent attempts by the federal government to try and gain the upper hand in the face of a growing cybersecurity threats. Other recent federal government actions in this area include a new DOJ initiative to combat poor government contractor cybersecurity practices and new breach notification requirements for banks and their service providers.

Covered Entities

The new critical infrastructure law requires "covered entities" to report any "covered cyber incident" to CISA no later than within 72 hours after the entity reasonably believes that a covered cyber incident occurred.

Covered entity is broadly defined in the law to include any entity within a critical infrastructure sector, as defined in the Presidential Policy Directive 21. That directive lists the following critical infrastructure sectors: (1) chemical; (2) commercial facilities; (3) communications; (4) critical manufacturing; (5) dams; (6) defense industrial base; (7) emergency services; (8) energy; (9) financial services; (10) food and agriculture; (11) government facilities; (12) healthcare and public health; (13) information technology; (14) nuclear reactors, materials, and waste; (15) transportation systems; and (16) water and wastewater systems. Additionally, whether an entity (and their services or products) are considered critical infrastructure depends on it "the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

These sectors can include banks, financial industry service providers, hospital systems, healthcare service providers, telecommunication providers, internet service providers, and transportation service providers.

Per the above, the potential applicability of the law is extremely broad, and its full scope will be unknown until CISA publishes a final rule better delineating the factors used in determining whether an entity needs to comply with the law.

However, the new law provides some guidance to CISA in its rulemaking process, specifically in defining "covered entity." CISA must consider: (1) the consequences that a cybersecurity attack on a given entity will have on national security, economic security, or public health and safety; (2) the likelihood a given entity will be targeted by malicious actors; and (3) the damage or disruption such an attack on a given entity would have on the reliable operation of critical infrastructure.

Entities that potentially fall within the above 16 categories and provide broad services for a broad portion of the U.S. should pay close attention to, and engage in, the CISA rulemaking process.

Covered Cyber Incident

If an entity is in fact considered a covered entity, the second step in determining whether the law is triggered. Meaning, the entity must determine if the actual cybersecurity incident falls within the definition of a "covered cyber incident".

Under the new critical infrastructure law, a covered cyber incident includes any substantial cyber incident that a covered entity experiences. In line with the definition of covered entity, this is broadly defined as well and its full scope will be unknown until CISA publishes its final rule to better define when the reporting requirements are triggered. However, similar to the rulemaking process for defining "covered entity," the new law also explicitly provides guidelines for CISA's rulemaking.

The new law states that in determining the final rule's definition of a "covered cyber incident" CISA must consider: (1) the sophistication or novelty of cybersecurity attacks, and their type, volume, and the data subject to such attacks; (2) the number of persons impacted (directly or indirectly) by such attacks: and (3) potential impacts on industry controls (e.g., programmable logic controls).

Reporting Requirements

There are two main requirements under the new critical infrastructure law that place obligations on entities that fall within the law's scope.

First, if an entity is subject to a substantial "covered cyber incident," they must report that incident to CISA within 72 hours. Specifically, the reporting requirement is triggered, and the clock runs, when the entity reasonably believes a covered cyber incident occurred. Therefore, even when the entity is not 100% certain the incident occurred, the reporting requirement may be triggered.

Second, an entity must report to CISA within 24 hours if they make a ransomware payment pursuant to a ransomware attack.

Finally, the new critical infrastructure law also requires subsequent reports to be filed to CISA if substantial new or different information becomes available pursuant to the related cybersecurity event. It's important to note that, under the new law, third party providers are allowed to submit the foregoing reports on an entity's behalf.

Looking Ahead

With the full scope of the new law unknown, but the potential for broad applicability, any entity that believes it could fall under the new law's requirement should engage in CISA's rulemaking process, paying particular attention to the laws guidelines to CISA in shaping and defining the laws scope.

In light of the federal government's many recent efforts to combat cybersecurity incidents, ransomware attacks, and data breaches generally, CISA will likely aim for broad definitions and broad applicability.

As the federal government continues to combat the rise of major cybersecurity incidents and ransomware attacks, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Related Practices

Intellectual Property

Data Privacy & Cybersecurity

Related Professionals

Ryan T. Sulkin
Partner Intellectual Property; Data Protection Group Lead
Intellectual Property
T. 312.624.6398
rsulkin@beneschlaw.com

Luke Schaetzel
Associate
Intellectual Property
T. 312.212.4977
lschaetzel@beneschlaw.com