Akin Gump
STRAUSS HAUER & FELD LLP

President Biden Signs Sweeping Cyber Legislation into Law

Key Points

- Under legislation signed into law today by President Joe Biden, certain companies will be required to report cyberattacks to the federal government within 72 hours, and ransomware payments within 24 hours.
- Within 24 months, the CISA is directed to publish an NPRM to implement the bill, followed by the issuance of a final rule within 18 months of the NPRM.
- This Alert summarizes the key takeaways for affected companies in order to prepare for the new requirements.

On Thursday, March 10, the Senate passed the fiscal year (FY) 2022 omnibus spending package to fund the government through September 2022, readying the bill for President Biden's signature. The final bill notably contains cyber incident reporting provisions which previously passed the Senate by unanimous consent on March 1 as part of the bipartisan Strengthening American Cybersecurity Act (S. 3600).

Reporting Requirements

The sweeping legislation requires covered infrastructure owners and operators to report cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. Additionally, the measure requires covered entities to report ransomware payments within 24 hours. Should "substantial" new or different information becomes available, such entities must also submit supplemental reports to the agency. The bill stipulates that covered entities may use a third party to submit a report.

Covered Entities

"Covered entities" are defined to include entities in a critical infrastructure sector, as defined in Presidential Policy Directive 21, which identifies 16 critical sectors and designates. The term "critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security,

Contact Information

If you have any questions concerning this aler, please reach contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Ed Pagano
Partner
epagano@akingump.com
Washington, D.C.
+1 202.887.4255

Taylor Daly
Policy Advisor
tdaly@akingump.com
Washington, D.C.
+1 202.416.5541

national economic security, national public health or safety, or any combination of those matters."

Within 24 months, the CISA is directed to publish a notice of proposed rulemaking (NPRM) to implement the bill, followed by the issuance of a final rule within 18 months of the NPRM. Covered entities must also satisfy the definition established by CISA in its final rule, which will also outline the manner and form of reports, in addition to effective dates for such reporting requirements. Following promulgation of a final rule, the bill directs CISA to conduct an outreach and education campaign to inform likely covered entities of the rule's requirements.

Covered Incidents

In determining which types of entities are covered, the bill stipulates that the following will be considered:

- The consequences that compromise of such an entity could cause to national security, economic security or public health and safety.
- The likelihood that such an entity may be targeted by a malicious cyber actor.
- The extent to which damage, disruption or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure.

Further, the bill clarifies that the final rule must consider the following when determining whether a cyber incident constitutes a covered incident:

- The sophistication or novelty of the tactics used to perpetrate the incident, as well as the type, volume and sensitivity of the data at issue.
- The number of individuals affected or potentially affected by such a cyber incident.
- Potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems and programmable logic controllers.

Agency Requirements

Within 24 hours of receiving information related to a covered incident, CISA's National Cybersecurity and Communications Integration Center (NCCIC) must share the information with the appropriate Sector Risk Management Agencies (SRMAs) and other appropriate federal agencies.

The bill also directs NCCIC to, among other things:

- Receive reports from covered entities related to a covered incident to assess the effectiveness of security controls.
- Share information with appropriate federal agencies to track ransom payments.
- Leverage information gathered about cyber incidents to enhance information sharing.
- Facilitate the sharing, on a voluntary basis, between critical infrastructure owners and operators of information relating to covered cyber incidents.
- Publish quarterly unclassified reports outlining findings and recommendations.

CISA is directed to deploy a ransomware vulnerability warning pilot program to develop procedures for identifying information systems that contain security vulnerabilities associated with common ransomware attacks. In addition, the bill directs the Director of CISA to establish and chair the Joint Ransomware Task Force, consisting of participants from other federal agencies, also directing the U.S. Department of Homeland Security (DHS) to lead an intergovernmental Cyber Incident Reporting Council to harmonize federal incident reporting requirements, including those issued through regulations.

Enforcement

In the event that a covered entity fails to comply with the requirement to report, DHS may obtain information about the incident by engaging the covered entity directly to request information, or, if still unable, by issuing a subpoena. Further, if DHS has reason to believe that a covered entity has experienced a covered incident but failed to report it, the Secretary may request additional information. If DHS has not received a response within 72 hours of the request, the Secretary may issue a subpoena to compel disclosure of information. If an entity fails to comply with a subpoena, order, or inspection notice, the Secretary may bring a civil action in a district court to enforce the subpoena, order or notice.

Should DHS determine that the facts surrounding the incident may constitute grounds for a regulatory enforcement action or criminal prosecution, DHS may provide such information to the Attorney General or the appropriate regulator, who may use such information for a regulatory enforcement action or criminal prosecution.

Liability Protections

While the bill provides that no court may maintain a cause of action against any person or entity on the sole basis of submitting a report, the liability protections apply only to litigation that is based on the submission of a report or ransom payment to CISA, meaning that other Sector Risk Management Agencies collecting reports on cyber incidents will need to coordinate with CISA to determine how such information should be collected.

Conclusion

Looking ahead, it will be important for businesses to closely monitor for additional guidance from CISA in accordance with the bills' prescribed deadlines, as these rules will ultimately determine the effective date of the law's reporting requirement, in addition to the entities that will fall under the scope of the rules and the manner in which reports must be submitted.

akingump.com