SQUIRE PATTON BOGGS

Practical Takeaways From President Biden's Cyber Incident Reporting for Critical Infrastructure Act

US – April 2022

On March 15, 2022, President Biden signed into law the "Cyber Incident Reporting for Critical Infrastructure Act of 2022" (the Act). Since then, state, local, tribal and territorial entities, as well as public and private owners and operators of critical infrastructure, have been pouring over the legislation trying to understand its application and implications for, not only their organization, but also their respective industries. For that reason, what follows are answers to common questions.

Why Is the Federal Government Now Implementing Cybersecurity Legislation for Critical Infrastructure?

In early May 2021, Americans were riveted by scenes of panic buying at the pump after a ransomware attack shutdown the Colonial Pipeline, a critical source of fuel for the entire East Coast. For the first time, many reflected on the national security implications of cybersecurity attacks on everyday life – and the US government swiftly responded. By May 12, 2021, President Joe Biden signed an Executive Order on "Improving the Nation's Cybersecurity," as an almost demarcation line to modernize the federal government's cybersecurity practices – leading to expansive rules and enforcement of existing cybersecurity authorities. Now, in the wake of the Ukrainian conflict, where Russia has already used Ukraine as a testing ground for powerful cyber weapons, the Act finally received bipartisan Congressional support, after failing to pass similar legislation in recent years.

What Is the General Purpose of the Act?

In general, among other things, the purpose of the Act is to provide the Cybersecurity & Infrastructure Security Agency (CISA) with current and actionable information on cybersecurity attacks on critical infrastructure and the threat actors that perpetrated them in order to allow the Federal government to assess the threat and provide actionable guidance to various stakeholders to help mitigate future cybersecurity attacks. Those stakeholders include, among others, critical infrastructure owners and operators, the private sector, other Federal agencies and state and local governments.

What Does the Act Require of a Covered Entity?

The Act creates four main obligations for covered entities: (1) report certain cybersecurity attacks known as "covered cyber incidents" to CISA within 72 hours of determining the existence of the same; (2) report ransomware payments to CISA within 24 hours; (3) provide supplemental information if substantial or new information becomes available; and (4) preserve data relevant to the covered cyber incident.

While not a requirement, non-covered entities may voluntarily report cyber incidents or ransomware payments to CISA as a means to enhance CISA's situational awareness of cyber threats. Likewise, covered entities may voluntarily include additional information to CISA that is not required to be reported.

Does the Act Apply to My Organization?

While the application of the Act to private and public companies, as well as state, local, Tribal, and territorial government entities, is still under development by the Director of CISA (the Director), such entities can preliminarily assess the likelihood of application to their organizations.

First, at a minimum, the Act only applies to organizations that operate within one of the 16 critical infrastructure sectors, as defined in Policy Directive 21. A full list of those sectors is provided on CISA's website here.

Second, the Act appears to focus only on those organizations whose disruption resulting from a cybersecurity attack would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Accordingly, the Act requires that the Director promulgate rules that define whether an entity falls within a critical infrastructure sector, by broadly considering the following:

- The consequences of a disruption or compromise of the entity's operation would have on national security, economic security, or public health and safety
- The likelihood of the entity becoming a target of a cyberattack
- The extent a cybersecurity attack on the entity would disrupt the reliable operation of critical infrastructure

Entities can, therefore, use this criteria to preliminarily assess whether their organization will likely be included in the definition of "covered entity."

What Constitutes a Reportable "Covered Cybersecurity Incident"?

The Act requires the Director to create a clear description of the types of substantial cybersecurity attacks that constitute a "covered cyber incident." While the Act provides specific guidelines and considerations to develop this definition, at a minimum, a reportable covered cyber incident will have to fall within one of three categories of harm:

- Substantial loss of the confidentiality or integrity of an information system or network, such as unauthorized access to and/or exfiltration of an organization's information
- A disruption of normal business operations, such as through a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability
- Either of the above caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise

The definition, however, will not include cyber incidents perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system or a threat of disruption or extortion.

What Does My Organization Need to Report for a Covered Cyber Incident?

While the Act requires the Director to create a clear description of the specific required contents of a report, the report must include, at a minimum: (1) A description of the covered cyber incident; (2) a description of the vulnerabilities exploited and the security defenses that were in place prior to the covered cyber incident; (3) the tactics, techniques and procedures used to perpetrate the covered cyber incident; (4) if available, contact information and any other identifying information for the threat actor; (5) if available, the type of information compromised or reasonably believed to have been compromised; and (6) the organization's identification and contact information. Such information may be used by CISA and other agencies to mitigate cybersecurity harm and investigate and prosecute malicious cyber actors. Of course, this is the same type of information that plaintiffs and regulators seek to assess potential claims and/or regulatory enforcement actions. Fortunately, as detailed below, such information provided in a report is generally prohibited from such use.

What Does My Organization Need to Report for a Ransomware Payment?

While the Act requires the Director to create a clear description of the specific required contents of a report, the report must include, at a minimum: (1) a description of the ransomware attack; (2) where applicable, a description of the vulnerabilities, tactics, techniques and procedures used to perpetrate the ransomware attack; (3) where applicable, any identifying or contact information related to the threat actor; (4) the name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made; (5) the organization's identification and contact information; (6) the date of the ransom payment; (7) the ransom payment demand, including the type of virtual currency or other commodity requested, if applicable; (8) the ransom payment instructions; and (9) the amount of the ransom payment.

Note, if the covered cyber incident and the ransomware payment occur within 72 hours of determining the existence of a covered cyber incident, then only one report is required.

If My Organization Already Has to Report to One Federal Agency, Do I also Need to Report to CISA?

Maybe. Covered entities that are required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe may not need to submit a report to CISA, if an agency agreement and sharing mechanism is in place between CISA and the respective Federal agency. Accordingly, companies should identify existing reporting obligations and monitor interagency sharing agreements before reporting to CISA.

What Happens if My Organization Fails to Report?

The Act provides several enforcement mechanisms against private and public companies only (as state, local, tribal, or territorial entities are explicitly excluded). If a private or public covered entity fails to submit a required report, the Director may directly engage with the covered entity to gather sufficient information to determine whether a covered cyber incident or ransom payment has occurred. If the covered entity does not respond within 72 hours, or provides inadequate information, the Director may issue a subpoena. In the event that the covered entity does not respond to the subpoena, or provides inadequate information, the Director may refer the matter to the Department of Justice to enforce the subpoena. There, a court may punish a covered entity for its failure to comply with a subpoena as contempt of court.

More importantly, if the Director determines, based upon the information provided in the eventual response to a subpoena, that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency for regulatory enforcement action or criminal prosecution. In doing so, the Act incentivizes timely reporting. Accordingly, private and public companies should, at a minimum, ensure that it has the appropriate policies and procedures in place to ensure that it meets any notification obligations in a timely manner.

Can Timely Reported Information Be Used Against My Organization?

To mitigate understandable concerns related to reporting, the Act protects reporting entities, including those that reported voluntarily, from enforcement actions associated with the content of the reports. Under the Act, the contents of the reports cannot be used by CISA, other federal agencies, or any state or local government to regulate, including through enforcement action, the activities of the covered entity that submitted the report. This exemption does not apply, however, if the covered entity is reporting to CISA to meet regulatory reporting obligations based upon an agency agreement and sharing mechanism between CISA and the respective Federal agency. This exemption also does not apply in the event that the CISA Director refers the matter to the Department of Justice to enforce the subpoena against the covered entity. Further, the contents of the report may be used to inform the development of future regulations and their implementation.

The Act also protects reporting entities, including those that reported voluntarily, from certain liability associated with the filing of the reports. In particular, no cause of action can be maintained based "solely" on the submission of a report (unless it is an action taken by the federal government to enforce a subpoena against a covered entity.) Further, the required reports, and material used to prepare the reports, cannot be received as evidence, subject to discovery, or used in any proceeding in federal or state court or before a regulatory body.

Finally, submitted reports:

- Do not constitute a waiver of any applicable privilege or protection provided by law
- Must be exempt from disclosure under freedom of information laws and similar disclosure laws
- Cannot be subject to a federal rule or judicial doctrine regarding *ex parte* communications
- Must be considered commercial, financial and proprietary information if designated

In doing so, these provisions are meant to further encourage compliance and mitigate the concerns that victim organizations may face in providing notifications.

When Will the Act Go Into Effect?

The obligations for covered entities will go into effect on the date set by the Director in the final rule. The legislation requires the Director to develop the final rule in consultation with Sector Risk Management Agencies, the Department of Justice, and other federal agencies. The Director has 24 months to publish the notice of proposed rule to the Federal Registrar and thereafter another 18 months to issue a final rule. Once the final rule is issued, CISA will conduct an outreach and education campaign to inform likely covered entities and supporting cybersecurity providers of the Act's requirements.

What Should I Do Now to Prepare?

It has arguably never been more critical for organizations to assess their preparation to mitigate the risk of and respond to a cybersecurity incident. Since President Biden's May 2021 Executive Order, where he promised to make cybersecurity the highest priority of his administration, we have seen regulators double-down on enforcing existing cybersecurity laws and promulgating proposed rules to expand their authority to enforce the same.

Likewise, where Russia has already used Ukraine as a testing ground for powerful cyber weapons, the Administration will likely continue to make cybersecurity a focus of its national security agenda. Once more, the FBI has recently warned that US critical infrastructure has been subject to reconnaissance for cyberattacks. For these reasons and others, President Biden has called upon companies' patriotic obligation to prepare for cybersecurity attacks. As such, it would be prudent for any organization to assess its cybersecurity posture and ensure that it has implemented industry best practices, to the extent practical. At a minimum, to maximize the protections afforded by the Act, an organization should ensure that it has the appropriate policies and procedures in place to meet its reporting obligations in a timely manner.

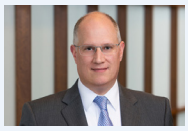
Contacts

Ericka A. Johnson
Senior Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com

Ericka Johnson responds to global and domestic ransomware attacks and data breaches on behalf of clients across a variety of industries (e.g., automotive manufacturing, insurance, mining, higher education, legal, financial and health care). In particular, Ericka has extensive experience working with IT forensic firms to help her clients understand and meet their various legal obligations. She frequently interfaces with law enforcement and industry-specific regulators in the US and coordinates filings with and responses to inquiries from regulators around the world (e.g., EU, South Pacific, Africa and Latin America).

Ericka regularly assists clients with cyber risk mitigation strategies. She frequently conducts cybersecurity risk assessments against various cybersecurity standards and develops internal compliance measures and incident response protocols to remediate identified vulnerabilities.

Prior to joining private practice, Ericka served for six years as Judge Advocate in the US Marine Corps, where she specialized in, among other things, cyber operations. She continues to serve as reserve operations officer to the Judge Advocate commanding general in the Washington DC area.



Colin R. Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Colin Jennings has been selected as primary outside counsel for global compliance work by more than 35 public and privately held global companies, and regularly provides guidance and counselling in connection with these companies' ongoing compliance efforts for both their domestic and international operations, including, when necessary, investigation of compliance-related concerns.

He regularly interacts with federal, state and international authorities concerning data breaches, and coordinating the forensic analysis and resulting claims or litigation that inevitably follow a breach. As the currently appointed cyber lawyer for the state of New Jersey, he has helped multiple jurisdictions, both in and out of the state, develop the requisite policies, procedures and trainings to prepare for, and respond to, cyberattacks.

Colin regularly conducts compliance reviews and internal investigations domestically and abroad. His advice on the design, implementation and assessment of compliance programs is informed by internal investigations. He has conducted investigations into allegations of employee theft, fraud or other business misconduct, including alleged violations of the Foreign Corrupt Practices Act (FCPA), sanctions and export control violations, and has experience litigating claims arising from compliance-related matters.