Freeborn

Strengthening American Cybersecurity Act: For Many, a 72 Hour Notification Deadline is Coming

by Joel B. Bruckman

A FREEBORN & PETERS LLP CLIENT ALERT

Overview

On March 15, 2022, President Biden signed into law the Strengthening American Cybersecurity Act ("SACA"), which includes the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Act"). The Act created a framework for reporting obligations with a 72-hour notification deadline for victims of cyber-attacks whose businesses operate in certain "critical infrastructure sectors." Oversight and enforcement of compliance will be handled by the Cybersecurity and Infrastructure Security Agency ("CISA") in conjunction with the Department of Justice ("DOJ"). Although the Act has been signed into law, the director of CISA has 24 months to publish a notice of proposed rulemaking and permits an additional 18 months thereafter for issuance of a Final Rule.

Who Constitutes a Covered Entity?

At this point, while we await the Final Rule and its definition of what constitutes a "Covered Entity" for purposes of the Act, Presidential Policy Directive 21 has defined Critical Infrastructure industries as including the following:

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
16. Water and Wastewater Systems

What Triggers Notification?

The Act provides that "at a minimum" the following shall constitute "substantial cyber incidents" to be covered by the Act:

- A cyber incident that leads to a substantial loss of confidentiality, integrity, or availability of such information system or network or a serious impact on the safety and resiliency of operational systems and processes.
- A disruption of business or industrial operations, including a denial of service attack, a ransomware attack, or exploitation of a zero-day vulnerability against an information system or network, or an operational technology system or process.

- Unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, a managed service provider, or another third-party data hosting provider, or by a supply chain compromise.

The Act further provides that you are to consider: "i) the sophistication of novelty of tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue; ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and iii) potential impacts on industrial control systems."

Notification Timeline

Once a cyber incident has been discovered, a Covered Entity has 72 hours to provide initial notification to CISA. Failure to comply may subject a Covered Entity to being the target of a subpoena from CISA and/or referral for investigation to the Department of Justice.

Use This Time to Prepare and Get Your Incident Response Plan in Order

- Do you have an Incident Response Plan to allow you to effectively and efficiently respond to a data security incident? If not, we can help you prepare an Incident Response Plan. If you already have one, when did you last review and update it? We can also assist you in updating your current Incident Response Plan to ensure that it is up to date and contemplates the most recent legal notification obligations.

- Have you put your Incident Response Plan to the test? Let us run a table-top exercise to see how your team responds to a cybersecurity crisis, identifying areas of improvement so that you are ready for the "real thing."

- What about the implementation of i) administrative, ii) physical, and iii) technical safeguards to protect your sensitive data: Have you created such safeguards with a mind towards cybersecurity? When were those safeguards last reviewed and strengthened? Regulators scrutinizing your response to a data security incident will focus on that very question and your efforts to determine whether you took reasonable steps to avoid a breach of sensitive data.

Working together we can prepare you for what's coming, SACA and beyond…

If you have any questions, please contact Joel Bruckman at (312) 360-6461 or jbruckman@freeborn.com, or another member of Freeborn's Cybersecurity and Data Privacy Team.

Freeborn

ABOUT THE AUTHOR

Joel B. Bruckman

Partner

Chicago Office
(312) 360-6461

jbruckman@freeborn.com

Joel is a Partner in the Litigation Practice Group and a member of the Insurance/Reinsurance Industry Team and the Emerging Industries Team. He has extensive experience in White-Collar criminal investigations and post-indictment matters including allegations of Fraud, Theft, Embezzlement, Money Laundering and Anti-Trust Violations under The Sherman Act, Wire Fraud and private-sector Honest Services Fraud. As a former member of the FBI's Cyber Crimes Task Force during his time as a prosecutor for the Cook County State's Attorney's Office, Joel regularly advises clients on data security incident response strategies and best practices, from initial discovery and computer forensics investigations through statutory / regulatory notification compliance and subsequent government investigation and private-party litigation.

130+ Attorneys.
5 Offices.

Freeborn & Peters LLP is a full-service law firm with international capabilities and offices in Chicago, Ill.; New York, Ny; Richmond, Va.; Springfield, Ill.; and Tampa, Fla. Freeborn is always looking ahead and seeking to find better ways to serve its clients. It takes a proactive approach to ensure its clients are more informed, prepared and able to achieve greater success – not just now, but also in the future. While the firm serves clients across a very broad range of sectors, it has also pioneered an interdisciplinary approach that serves the specific needs of targeted industries.

Freeborn's major achievements in litigation are reflective of the firm's significant growth over the last several years and its established reputation as a Litigation Powerhouse®. Freeborn has one of the largest litigation departments among full-service firms of its size – currently with more than 90 litigators, which represents about two-thirds of the firm's lawyers.

Freeborn is a firm that genuinely lives up to its core values of integrity, effectiveness, teamwork, caring and commitment, and embodies them through high standards of client service and responsive action. Its lawyers build close and lasting relationships with clients and are driven to help them achieve their legal and business objectives.

For more information visit: www.freeborn.com

CHICAGO
311 South Wacker Drive
Suite 3000
Chicago, IL 60606
(312) 360-6000
(312) 360-6520 fax

NEW YORK
1155 Avenue of the Americas
26th Floor
New York, NY 10036
(212) 218-8760
(212) 218-8761 fax

SPRINGFIELD
217 East Monroe Street
Suite 202
Springfield, IL 62701
(217) 535-1060
(217) 535-1069 fax

RICHMOND
901 East Byrd Street
Suite 950
Richmond, VA 23219
(804) 644-1300
(804) 644-1354 fax

TAMPA
1 Tampa City Center
201 North Franklin Street
Suite 3550
Tampa, FL 33602
(813) 488-2920