wiley

NEWSLETTER

The Private Sector Should Brace for New Mandatory Cyber Incident Reporting Obligations

March 2022

Privacy In Focus®

Late 2021 and early 2022 have been full of federal government activity related to cybersecurity incident reporting. Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 to require mandatory reporting by critical infrastructure of substantial cyber incidents and ransomware payments within tight timeframes. The U.S. Securities and Exchange Commission (SEC) just proposed new cybersecurity rules for publicly traded companies to enhance and standardize public cybersecurity disclosures. These proposals come on the heels of Security Directives from the Transportation Security Administration (TSA) which imposed mandatory reporting on rail and pipeline sectors. The new cyber incident reporting legislation, as well as certain previous mandates, require reporting cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS).

Many private sector entities are wondering how these mandates relate to each other, whether they overlap, and how the information required may differ. Public companies in critical infrastructure may face multiple reporting obligations, with different triggers and different timelines. Wiley has repeatedly advised that the government is increasingly requiring the private sector to enhance cybersecurity through these disclosure obligations and cyber incident reporting mandates. Wiley has also been advising clients to implement sound cybersecurity risk management processes now as we help them navigate these new legal and regulatory challenges.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

As companies try to anticipate their obligations, they should pay careful attention to the government's deadlines and reporting requirements and seek to avail themselves of available liability or disclosure protections where possible. Many in the private sector have been providing information to DHS under the Cybersecurity Information Sharing Act of 2015, which afforded protections to certain information voluntarily shared under the Act. Wiley recommends that cybersecurity incident response plans and crisis management plans be updated to expressly account for new government reporting obligations, available protections, and deadlines.

Private sector entities may want to urge policymakers to simplify and deconflict reporting obligations, particularly while the SEC and DHS engage in rulemaking for cybersecurity incident reporting. As the private sector seeks to understand the rapidly shifting landscape of reporting and disclosure obligations involving cybersecurity incidents, ransomware attacks, and data breaches, the chart below contains a useful summary of key attributes of new and proposed reporting in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the SEC's proposed cybersecurity rules for publicly traded companies, and the currently applicable TSA Security Directives. Subsequent rulemaking (with an opportunity for public comments) will further define these obligations.

Wiley's Privacy, Cyber & Data Governance team has been advising clients for over a decade on cyber risk management and data security. This includes cybersecurity incident response as well as incident and data breach reporting under federal and state law, including Gramm-Leach-Bliley, CISA 2015, the Customer Proprietary Network Information regime, and regulations for the Defense Industrial Base and government contractors, among others. Wiley helps organizations comply with recent government reporting requirements, plan for compliance with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and proposed SEC rules, and obtain protections under the program for Protected Critical Infrastructure Information and CISA 2015. We urge clients to proactively build relationships with the Federal Bureau of Investigation (FBI) and DHS, as we enter a new phase of public-private collaboration that includes disclosure obligations and penalties for cybersecurity deficiencies. Please contact Megan L. Brown, Jacqueline F. "Lyn" Brown, Jon W. Burd, Duane C. Pozza, Kathleen E. Scott, or Joan Stewart with questions or for advice.

Agency

Status of Obligation

Who Must Report?

What Triggers an Obligation to Report?

To Whom?

What Information Must Be in a Report?

What Are the Deadlines?

DHS

Cyber Incident Reporting for Critical Infrastructure Act of 2022; mandates reporting and directs DHS to make rules to clarify reporting obligations

Entity* in one of the 16 critical infrastructure sectors

"reasonable belief" that a "substantial" cyber incident occurred;

Reportable incidents include:

- Substantial loss of confidentiality, integrity, or availability of a system or network;
- Serious impact on operational systems and processes;
- Disruption of business or industrial operations.

DHS

CISA

- Function of the systems affected;
- Type of unauthorized access;
- When the incident took place;
- Operational impact;
- Any identifying information about the perpetrators;
- Known vulnerabilities exploited; and
- Identifying and contact information about the victim organization.

Within **72 hours of covered incident**

Update covered incident reports "promptly" if "substantial new or different information" becomes available.

Notify CISA when incident "has concluded and been fully mitigated and resolved."

DHS

Cyber Incident Reporting for Critical Infrastructure Act of 2022; mandates reporting and directs DHS to make rules to clarify obligations

Entity* in one of the 16 critical infrastructure sectors

A ransom payment for a "ransomware attack"

Ransom defined as: "use of threat of use of unauthorized or malicious code…or… another digital mechanism such as a denial of service attack, to interrupt or disrupt … or compromise … an information system *to extort a demand for a ransom payment*".

DHS

CISA

- Description of ransomware attack, including estimated date range;
- Description of tactics, techniques and procedures;
- Date and amount of ransomware payment, including the virtual currency or commodity requested;
- Ransom instructions including virtual currency or physical address to send funds;
- Any identifying information about the perpetrators; and
- Identifying and contact information about the victim organization.

Within **24 hours of ransom payment**

Must file new report if ransomware incident becomes "substantial," even if already reported ransom payment.

SEC

Proposed rule March 9, 2022; comments due May 9, 2022 or after 30 days publication in Federal Register, whichever is later

Public companies

"material cybersecurity incident"; materiality is based on existing standard, may include the nature, extent, or potential magnitude of an incident, and harm to company's reputation, financial performance, customer and vendor relationships, and litigation or regulatory risk.

SEC (Form 8-K,
6-K,
20-F)

- When incident discovered and if ongoing;
- Brief description of nature and scope;
- Whether any data stolen, altered, accessed, or used for unauthorized purpose;
- Effect of incident on registrant operations;
- Whether incident is remediated or being remediated.

Within **4 business days** of determination of a material cybersecurity incident; materiality determination must be made "as soon as reasonably practical"; update report in 10-Q or 10-K.

TSA

Security Directives effective December 31, 2021

Freight and passenger railroad carriers, rail transit operators

Cybersecurity incidents on IT or OT systems including:

- Unauthorized access
- Malware
- Denial of service
- Any other cyber incident that results in operational disruption, or
- Has the potential to impact large numbers of customers, critical functions, or public health/ national security

DHS

CISA

- Affected systems or facilities, including location;
- A description of the incident;
- Any known threat information including about the perpetrator, if available; and
- A description of the impact or potential impact on operations or systems, including:
  - Assessment of actual or imminent adverse impacts to service, such as delays;
  - Whether data theft has or is likely to have occurred; and
  - Any other information that would be useful in understanding the impact or potential impact of the incident.
- Summary of planned or considered responses (e.g. revert to manual switch operation).

Within **24 hours of identifying** the cybersecurity incident

Update if required information becomes available that was not available at the time of the report.

**Entities in the 16 critical infrastructure sectors currently include: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care/public health, information technology, nuclear reactors/materials/waste, transportation, and water/wastewater systems.*