wiley

NEWSLETTER

Cyber Reporting Considerations

November 2025

The regulatory environment has transformed cybersecurity failure into a core legal, financial, and compliance risk. Today, organizations must navigate a complex maze of conflicting deadlines across state and federal jurisdictions. This means, in addition to directing the incident response, organizations should implement processes to track decision-making and be prepared to meet all reporting requirements that may apply. To preserve privilege, organizations may consider dual-tracking cyber incident investigations with one directed by counsel focused on the regulatory and legal aspects of investigations that would be "in anticipation of litigation" and another that would be conducted in the normal course of business. Organizations should be aware of the varied applicable requirements and deadlines, along with the liability considerations and increased accountability they impose. Examples include:

1. Conflicting Deadlines

Multi-jurisdictional incidents trigger non-uniform reporting clocks that can challenge organizations. As a result, incident response must include tracking a strict timeline for compliance. For example:

- Defense Federal Acquisition Regulation Supplement (DFARS): The incident response is governed by a stringent clock – the DFARS 72-hour mandate, which requires "rapidly report[ing]" any cyber incident affecting *covered* defense systems, information, or services within 72 hours of discovery. Crucially, DFARS non-compliance creates a risk of False Claims Act (FCA) enforcement, as the knowing failure to implement required security or report within 72 hours can be viewed as procurement fraud.

Authors

Erin M. Joe
Special Counsel
202.719.3140
ejoe@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance

- New York Department of Financial Services (NY DFS): The New York Department of Financial Services requires covered entities to notify the Department within 72 hours of determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider. (23 NYCRR Part 500.17(a))
- Securities and Exchange Commission (SEC): The SEC requires public companies to disclose a cyber incident within four business days of determining the incident would be material to a reasonable investor. This framework forces legal and executive teams to conduct a swift, accurate materiality analysis to mitigate the risk of enforcement for delayed disclosure.
- Health Insurance Portability and Accountability Act (HIPAA): Under HIPAA, notification is required for breaches of unsecured protected health information (PHI) within a maximum of 60 days from discovery, but emphasizes that notification must be made "without unreasonable delay," leading to penalties for delaying the process even within the 60-day limit.

2. Accountability Through Executive Certification

Regulators are mandating proactive security controls placing, direct liability on leadership for the integrity of their cybersecurity programs in the form of proactive reporting, attestation, and/or certifications, which raise potential liability for the submitting businesses. For example:

- DFARS: Compliance is formalized and now requires an annual affirmation of continuous compliance with Cybersecurity Maturity Model Certification (CMMC) program requirements. The "affirming official" must be a representative authorized to speak for the organization. Knowingly submitting a false affirmation creates a clear path for FCA enforcement. Compliance is required prior to contract award and extends to subcontractors. So, it is advisable for contractors to verify the compliance of their subcontractors or ensure subcontractors are not handling the covered information.
- California Consumer Privacy Act (CCPA): California will begin requiring businesses to submit an attestation confirming that mandated privacy risk assessments have been completed. While there are several deadlines depending on the activity, compliance with new requirements begins as early as January 1, 2026. For covered processing that was initiated before January 1, 2026, and that continues after January 1, there is more time – in that scenario, assessments must be conducted and documented no later than December 31, 2027.

Compliance deadlines for conducting cybersecurity audits and submitting certifications are staggered based on a business's annual gross revenue. Large businesses with over $100 million in revenue for 2026 must complete their first audit by April 1, 2028, covering the period from January 1, 2027 to January 1, 2028. Medium businesses, earning between $50 million and $100 million in 2027, must complete their first audit by April 1, 2029, for the period from January 1, 2028 to January 1, 2029. Small businesses with less than $50 million in revenue for 2028 have until April 1, 2030, to complete their first audit, covering the period from January 1, 2029 to January 1, 2030. A certification of completion must be submitted to the California Privacy Protection Agency (CPPA), and businesses must retain audit records for a minimum of five years. The audits must be performed by a qualified, independent auditor who may be internal or external, but must report to

senior leadership not directly responsible for cybersecurity.

- NY DFS: Covered Entities must submit an annual certification of compliance regarding their cybersecurity program maturity, risk assessment, and incident response plan readiness, forcing continuous review.

3. Effective Risk Management

When outsourcing data processing, the primary organization often remains liable under the applicable regulations. Effective risk mitigation requires transparency with third-party vendors, which includes the following:

- Mandating the Right to Audit: Consider requiring contracts that contain a robust "Right to Audit" clause that grants the authority to inspect a vendor's system and verify security compliance.
- Allocating Liability: Consider contract provisions that allocate responsibility for regulatory fines, penalties, and enforcement costs stemming from vendor data security violations.
- Requiring Third-Party Verification: Consider requiring auditing and verification that attests to the effectiveness of a vendor's security controls over time.

***

Wiley's Privacy, Cyber & Data Governance and Government Contracts teams collaborate closely to help entities of all sizes from various sectors proactively address risks and compliance with evolving privacy, cybersecurity, and federal procurement regulations, and advocate before government agencies. Please reach out with any questions.

Spotlight on Erin Joe

Wiley recently welcomed Erin Joe, who brings two decades of leadership experience spanning cybersecurity, national security, and technology, along with insight from overseeing thousands of investigations. Before joining Wiley, Erin held senior roles at the FBI, Mandiant, and Google Cloud, where she led initiatives advancing cyber defense, intelligence integration, and threat mitigation in response to some of the nation's most pressing challenges. Her addition strengthens Wiley's Cyber Practice and enhances the firm's ability to guide clients through the most complex cybersecurity issues across both government and private sectors.