wiley

ALERT

# Cybersecurity in 2024: Ten Top Issues to Consider

January 2, 2024

As we enter the New Year, Wiley has looked back at the top cyber issues for 2023 and what they mean for 2024. Last year, we saw the rollout of the National Cybersecurity Strategy—which outlined a new era of cyber oversight—as well as an unprecedented effort to regulate cybersecurity, incident response, and reporting in a variety of ways—including new rules and mandates from the Securities and Exchange Commission (SEC), the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), Transportation Security Administration (TSA), Environmental Protection Agency (EPA), state regulators (California and New York in particular) among others. We saw a spike in interest in zero trust and software security. We helped respond to investigations and surveillance reform proposals. We also addressed ransomware attacks and attempts to impose liability on company executives for cyber-attacks.

As the cost of responding to cyber-attacks keeps mounting, federal and state regulators have responded with increased regulations and disclosure requirements enhancing the complexities associated with responding to ransomware attacks and data breaches. This is a key inflection point in cyber policy, as the federal government touts harmonization while agencies proceed in varied directions.

We have identified the top ten policy issues that clients and others should consider in 2024, including new regulations, whether zero trust and software assurance have staying power, surveillance issues, CISO roles and risks, the impact of new SEC cyber disclosure rules, and more.

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Of Counsel
202.719.4114
jfbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law


## Practice Areas

Privacy, Cyber & Data Governance

**1. Incident reporting mandates proliferate – will government really harmonize them?**

2024 may be the year that incident reporting mandates reshape the cyber landscape. Government agencies are layering new and varied rules on top of the existing patchwork of state breach reporting and are taking a variety of approaches that may complicate compliance.

The Department of Homeland Security (DHS) reportedly will release a draft of its 72-hour reporting requirements for critical infrastructure under the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) in the next month or so. The private sector, which already faces a patchwork of incident reporting mandates, is keenly interested in how these broad new rules will take shape. Already, CISA published a Request for Information (RFI) kicking off the CIRCIA rulemaking, and one issue that many companies seemed focused on concerned the logistics of reporting, as there are currently many different reporting forms and online portals in use by DHS, the Federal Bureau of Investigation (FBI), and others. CIRCIA gave DHS two years to develop the proposed rules and their issuance in the New Year will provide critical infrastructure entities and related trade associations with an important opportunity to comment on how the prospective new reporting obligations will impact their operations. We continue to urge critical infrastructure owners and operators to consider making comments on the new draft rules to help define which companies need to report what types of incidents.

A variety of other incident and breach reporting regulations continue to emerge from both the federal government and states. For example:

- New SEC cyber incident reporting rules took effect last month and require public disclosures of material cybersecurity incidents within 4 days for companies subject to filing Form 8-K's. The SEC's new breach reporting rules add to an already complicated cybersecurity landscape of federal and state regulations. The new rules have a narrow exception to the reporting requirement for public disclosures that harm national security or public safety, but new guidelines issued recently by the Department of Justice (DOJ) indicate that such delays will be granted sparingly and only in the most extraordinary of circumstances.
- In December, the FCC adopted controversial new data breach reporting obligations, mandating breach notifications to consumers, the FCC, and law enforcement for certain data breaches involving a broader range of data than the FCC has typically claimed authority over.
- A new set of requirements for reporting is being contemplated for federal government contractors, as well, with the government in October releasing draft rules for all government contractors, which uses an 8 hour trigger and has different definitions.
- And at the state level, in November, the New York Department of Financial Services (NYDFS) adopted amendments to its Cybersecurity Requirements for Financial Services Companies which add to the existing requirement for a covered entity to notify the agency no later than 72 hours after determining a cybersecurity incident has occurred. As of December 1, 2023, covered entities must notify NYDFS of certain ransomware incidents, and also are subject to a continuing obligation for the covered entity to update the agency with material changes or new information previously unavailable. NYDFS has also

expanded the scope of reportable cybersecurity incidents to those at a covered entity's affiliates or a third-party service provider.

Amidst this flurry of regulatory activity, the Biden Administration has taken steps to look at harmonizing cyber regulations. The Office of the National Cyber Director (ONCD), within the Executive Office of the President (EOP) released an RFI in July 2023 that sought comments on how to harmonize cybersecurity regulations. ONCD's RFI came during the continued onslaught of new cybersecurity proposals and expectations which create complex compliance burdens on organizations across a range of sectors, many of which are already subject to various other cyber incident reporting and regulatory obligations. The RFI offered stakeholders with an important opportunity to reiterate to the federal government the importance of harmonization and deconfliction in the cybersecurity arena.

Organizations will need to get a handle on all of these competing regulatory requirements. The flow of the multitude and varied number of confidential and public reporting requirements necessarily impacts how the regulators treat incidents and victims. All of this begs the question, what is the effect of the calls in Congress and in the Administration for meaningful harmonization of incident reporting, if agencies are doing different, overlapping and sometimes conflicting things?

As a result, companies may want to review their incident response plans now to build in early consideration of their respective reporting requirements and possible coordination with law enforcement regarding the prospects for public reporting delays based on threats to national security or public safety. Companies may also want to invest time before a cyber incident in working relationships with trusted counsel and internal security stakeholders, including in-house counsel, who can interact with government stakeholders, as appropriate, during an incident.

**2. New cyber mandates are coming – how far will requirements go?**

The government is seeking to "rebalance" responsibilities in cyber as described in the National Security Strategy released in March 2023. As a result, regulators are moving toward new substantive requirements, using varied approaches. DHS has developed Cross-Sector Cybersecurity Performance Goals, which were supposed to be voluntary but are being identified by regulators as part of new requirements. The FCC, for example, has imported them into new mandates for A-CAM program participants, while it also has begun requiring certifications of the use of the NIST Framework for Improving Critical Infrastructure Cybersecurity. Indeed, the FCC previews more cyber mandates in its proposed plan to reclassify broadband services as Title II, which it justifies in part by claiming potential benefits from future cyber regulation.

National security agencies and regulators partnered to offer recommendations for the private sector which called on technology manufacturers to take ownership of improving the security outcomes of their customers and to break the vicious cycle of creating and applying fixes. In October, the government released *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default*, with international peers, advising providers to implement "secure-by-default" designs and in some cases override customers' security choices. The move to recommending secure-by-design further highlights the government's

embrace of cybersecurity performance goals, originally developed for critical infrastructure, as setting an important bar for other sectors as well.

Other agencies are moving forward with operational and administrative mandates, like the third Security Directive released by the TSA for rail and an equivalent approach to pipelines and airport and aircraft operators.

States are actively regulating as well. For example, the updated NYDFS cybersecurity requirements mentioned above include substantive cybersecurity regulations, as well as incident reporting obligations. And California, through its newly established privacy agency, is in the preliminary stages of a rulemaking process to impose cybersecurity audit requirements on companies subject to the California Consumer Privacy Act (CCPA).

It remains to be seen how these regulations unfold—especially given the legal issues around authority that we discuss below—but for the time being, agencies appear to be heeding the National Cybersecurity Strategy's call for more regulation.

**3. Zero trust gets codified – is it a catch phrase or a concept with staying power?**

2023 brought attempts to codify "zero trust" as the government continued to promote the security concept and vendors started selling it. NIST and other parts of government, including the President's National Security Telecommunications Advisory Committee (NSTAC), began looking at zero trust years ago; the concept is that assets and users accounts should not be trusted based solely on their physical or network location or ownership is not new. In 2023, the phrase caught fire and in 2024 we expect to see mandates and demands from government to build and use zero trust systems. For example, Congress in the FY2024 National Defense Authorization Act (NDAA) directed the Department of Defense (DOD) to apply zero trust principles to cyber defense for nuclear command, control, and communications systems and networks.

Zero trust is a concept that applies in varied ways to different sectors. It is not an operational checklist or uniform framework and assurances of zero trust may be hard to measure or enforce. Given recent government emphasis on "accountability," zero trust may present compliance questions and challenges for regulated entities and contractors. In 2024, we will be watching how zero trust evolves, and whether it turns out to be a buzz word for familiar ideas, or if it has staying power in mandates and contract requirements. If the latter, we will be interested in how prescriptive and predictable those turn out to be.

**4. Software development and assurance mandates come to life—how will attestation issues be resolved?**

The Federal Government is developing requirements for vendors to demonstrate secure software development practices—a task assigned in the 2021 Executive Order 14028, *Improving the Nation's Cybersecurity*. CISA and the Office of Management and Budget (OMB) have moved forward with a common form for "Secure Software Development Attestation." To use vendor-provided software, Federal departments and agencies will have to obtain an attestation from the producer that it uses the National Institute of Standard's (NIST's) Special Publication (SP) 800-218: Secure Software Development Framework[1] and Software Supply Chain Security Guidance.[2] Numerous questions remain about the mechanics of attestation and its effects on government

contracts, with commenters on an April 2023 release of the draft form seeking clarity and recommending changes that were not addressed in the November 2023 release.[3] Once OMB approves the common form, which could happen in the first few months of 2024, agencies will have to collect attestations for "critical software" (as defined in OMB Memo M-22-18)[4] within three months of OMB approval, and within six months of OMB approval for all other software. This is in addition to two major pending rules for government contractors, described here.

In addition to forthcoming mandates for government contractors, the Cybersecurity and Infrastructure Security Agency (CISA) continues to emphasize its "Secure by Design" campaign. The agency and over a dozen international partners released an updated version of its Secure by Design white paper in October 2023,[5] and CISA has issued an RFI on the draft white paper, with comments accepted until February 20, 2023.[6] CISA continues to call for "strategic investment of dedicated resources by software manufacturers," and notes that its Secure by Design efforts are consistent with the National Cybersecurity Strategy's calls to shift costs and liability for vulnerabilities to companies that develop software. [7]

With mandates for government contractors coming soon, and the government continuing to emphasize changes to software development business practices, companies should be looking to assess their existing programs against government guidance, engage with the appropriate agencies to help them understand existing practices and tradeoffs, and consider expanding compliance programs to address new requirements.

**5. Surveillance issues will be prominent, from FISA Section 702 reauthorization to government network monitoring – how will government balance national security and privacy interests and protect compliant companies?**

FISA Section 702 reauthorization will get a lot of airtime in early 2024 as Congress takes up reauthorization again but as the discussions in late 2023 showed, these heated debates obscure other issues, including successes and useful tools for addressing cyber operations.[8]

It's important to our national security to ensure that the Intelligence Community can fulfil its vital mission of protecting the country in an increasingly dangerous world as geo-political tensions exploded on multiple fronts by the end of 2023. At the same time, U.S. person privacy interests need to be protected. Congress should also consider the needs of companies subject to this form of compulsory legal process. Companies on the receiving end of a FISA Section 702 directive want predictable standards and processes so that they understand whether they operate covered services and what they are expected to produce to the government. Companies also seek civil immunity from lawsuits when they respond to, and comply with, lawful government process in good faith.

While FISA Section 702 has been temporarily re-authorized through April 19, 2024, it remains to be seen whether Congress and the Executive Branch can find a way to ensure that our country continues to be protected from the types of foreign threats FISA Section 702 was intended to prevent.

At the same time, other cyber proposals may raise surveillance and civil liberties concerns of their own that justify scrutiny. For example, a pending proposal from the FAR Council would mandate government network access and monitoring rights, free from judicial review, in response to certain cyber incidents for government contractors. This could result in expansive government access to private systems that do far more than work on government contracts and have serious implications for personal information and private networks.

**6. Pressure and focus on CISOs continue – how will risks to CISOs expand?**

In a first for the SEC, the SEC charged a company's chief information security officer (CISO) with fraud for allegedly making misleading statements in SEC filings related to their company's known cybersecurity risks. The SEC's action likely previews the increased scrutiny that CISOs will face going forward. Among other things, the SEC's action emphasized that CISOs must have in place robust cybersecurity policies and procedures, be prepared to promptly escalate known security issues, document internal discussions, decisions and judgment calls in the event of an incident, and carefully review the accuracy of any public statements or disclosures about the breach.

This follows on the heels of another major company's CISO being sentenced to 3 years' probation and ordered to pay a fine of $50,000 for covering up a data breach involving millions of user records. During an FTC investigation of a data breach, the company reportedly was hacked again but the CISO attempted to have the hackers sign non-disclosure agreements and withheld information about the breach from the FTC. His prosecution and conviction sent shock waves through the CISO community. Are these just aberrations or will more CISOs find themselves under government scrutiny for their actions?

**7. SEC disclosures will influence public discussions of cyber incidents – will the new rules routinize partial information sharing or make companies embrace the unknown?**

The SEC's enforcement actions related to cybersecurity take on a new urgency in 2024. As we noted in December, the SEC's cyber incident disclosure rules became effective on December 18, 2023, and require public companies to file a public 8-K notice within 4 days of determining the company is experiencing a material cybersecurity incident. DOJ and the FBI have issued supplemental guidance indicating that companies will be able to obtain delays in public reporting for national security reasons only in limited circumstances, so public companies will have to make fast and accurate determinations about what information to disclose.

Now that the SEC rules are in effect, the press, regulators, and even criminals are closely watching for cybersecurity incident disclosure 8-Ks. Coverage of these disclosures is likely to drive significant public conversation about ongoing cybersecurity incidents. Notably, however, some of the first cyber incident disclosure 8-Ks filed after the rule went into effect have embraced uncertainty by disclosing that the company is experiencing a material cybersecurity incident, but that its impact and scope are or remain unknown.[9] Given that 4 days into a material cybersecurity incident, many companies will likely have only limited understanding of the impact and scope of an incident, this disclosure approach is likely to become and remain common, and is consistent with the SEC's guidance that victims "need not disclose specific or technical

information about [their] planned response to the incident or [their] cybersecurity systems, related networks and devices...."[10] The lack of available details early in an incident, however, also underscores the validity of many commenters' (and dissenting Commissioner's) concerns that 4 days is too short a time to require a public disclosure.[11] Companies will need to develop and practice their capabilities to produce the mandated disclosures in compliance with the SEC's rule amidst the atmosphere of uncertainty and disruption that material cybersecurity incidents bring.

**8. DHS/CISA will be put to the test as CIRCIA shifts the agency's role – how will this impact the private sector?**

As mentioned above, CIRCIA requires CISA to create broad new rules for critical infrastructure to report a "significant cyber incident" to CISA within 72 hours and report a ransomware payment within 24 hours. The parameters surrounding the reporting of incident and ransomware payments will be determined during the rulemaking. CISA is required to issue a Notice of Proposed Rulemaking (NPRM) within 24 months of enactment and a final rule within 18 months following the NPRM. CIRICA signals a significant shift in the role of CISA, which has not previously acted as a regulator of critical infrastructure and instead functions through collaboration and partnership with critical infrastructure particularly on cybersecurity.

The private sector should be watching how CISA defines the incident information required to be reported. An overly broad definition combined with an expansive scope of the contents required in incident reports could result in CISA collecting unmanageable amounts of data that bogs down analysis and sharing across critical infrastructure sectors, two of the key goals of CIRCIA.

CISA's ability to act as a partner collaborating to reduce critical infrastructure cyber risk may be impacted by CISA's implementation of the new regulations. In particular, the private sector should be interested in whether CISA will be able to manage these dual roles and whether critical infrastructure entities may be more reluctant to be forthcoming with sharing information on threats and mitigations through existing collaborative mechanisms.

**9. Courts may face tests of agency power – are agencies overstepping their statutory authorities?**

As federal departments and agencies follow the Administration's encouragement in the National Security Strategy to use existing authorities to put minimum cybersecurity standards in place, the private sector increasingly may question whether agencies are exceeding their lawful mandates.

For instance, in March 2023, the Environmental Protection Agency (EPA) tried to rely on the Safe Drinking Water Act to issue an "interpretive memo" indicating that its existing "sanitary survey" rules for states that include a requirement that the states evaluate the cybersecurity of operational technology during their audits of public water systems. The EPA also produced evaluation guides and associated materials in support of its memo but did not go through the formal NPRM process. Three states (Missouri, Arkansas, and Iowa) and two trade associations challenged the EPA rule in the 8th Circuit saying it was another attempt to push a rule through a memo instead of going through Congress in violation of the Administrative Procedure Act. The 8th Circuit stayed implementation of the EPA rule pending resolution of the challenge. As a result, the EPA

withdrew its memorandum. The White House has indicated it will ask Congress to enhance the EPA's authorities to be able to require states to conduct cybersecurity evaluations, but it isn't clear whether those attempts will be successful.

The litigation involving the EPA "rule memo" underscores that the approach of using emergency authorities or seeking to adapt existing authorities to new cybersecurity mandates may be tenuous. This raises questions about substantive security authorities being used to issue administrative mandates and/or circumvent the formal rulemaking process and may be just the beginning of challenges to agencies that are increasingly seeking to use their own authorities to impose *de facto* regulations upon the private sector without Congressional authorization first.

**10. How will AI and cyber policy interact as regulatory interest in AI explodes?**

Every regulator and legislator appears to be interested in artificial intelligence, with myriad proposals progressing at the state and federal level. The FCC, FTC, SEC and other agencies are looking at particular regulatory questions as dozens of workstreams were kicked off by a recent Executive Order, 14110, The *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. At the same time, Congress has dozens of draft bills and state legislatures and regulators are also taking action. For example, in 2023, California's new privacy agency previewed new AI-focused draft regulations, which we expect to be proposed and be open to public comment in the coming year.

Many of the reasons for interest invoke security issues. For example, many of NIST's directives under the EO 14110 deal with AI safety and security. Indeed, NIST closed out 2023 by publishing an RFI seeking comments on AI safety and security evaluation and auditing, red-teaming, and more. CISA has weighed in, stating that "security challenges associated with AI parallel cybersecurity challenges associated with previous generations of software that manufacturers did not build to be secure by design, putting the burden of security on the customer. Although AI software systems might differ from traditional forms of software, fundamental security practices still apply."

We set up a working group at Wiley to address cross-sector AI issues, and we are closely following for 2024 how regulators and legislators will address AI and whether cyber will drive new regulation of AI.

***

Wiley's Privacy, Cyber and Data Governance Team is engaged in all major cyber workstreams at the federal and state levels. We are helping clients prepare for new obligations and shape emerging frameworks and have been engaged in cyber policy for more than fifteen years, participating in almost every federal and state cyber policy development in 2023.

If you have questions about any of the issues above, or anything related to cyber, data security, network security, or privacy, please reach out to the authors here or your usual Wiley contact.

[1] https://csrc.nist.gov/pubs/sp/800/218/final.

[2] https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidanceunder-EO-14028-section-4e.pdf.

[3] https://www.regulations.gov/docket/CISA-2023-0001/comments.

[4] https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

[5] https://www.cisa.gov/resources-tools/resources/secure-by-design

[6] https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for

[7] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, Strategic Objective 3.3.

[8] *See, e.g., Expert Q&A with David Aaron on FISA Section 702 Reauthorization and Reform*, Just Security (Oct. 11, 2023), https://www.justsecurity.org/89387/expert-qa-with-david-aaron-on-fisa-section-702-reauthorization-and-reform/.

[9] https://www.wsj.com/articles/vans-north-face-parent-vf-warns-cyberattack-may-snarl-holiday-deliveries-93802dab?mod=djemCybersecruityPro&tpl=cy.

[10] https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214.

[11] https://www.sec.gov/news/statement/peirce-statement-cybersecurity-072623.