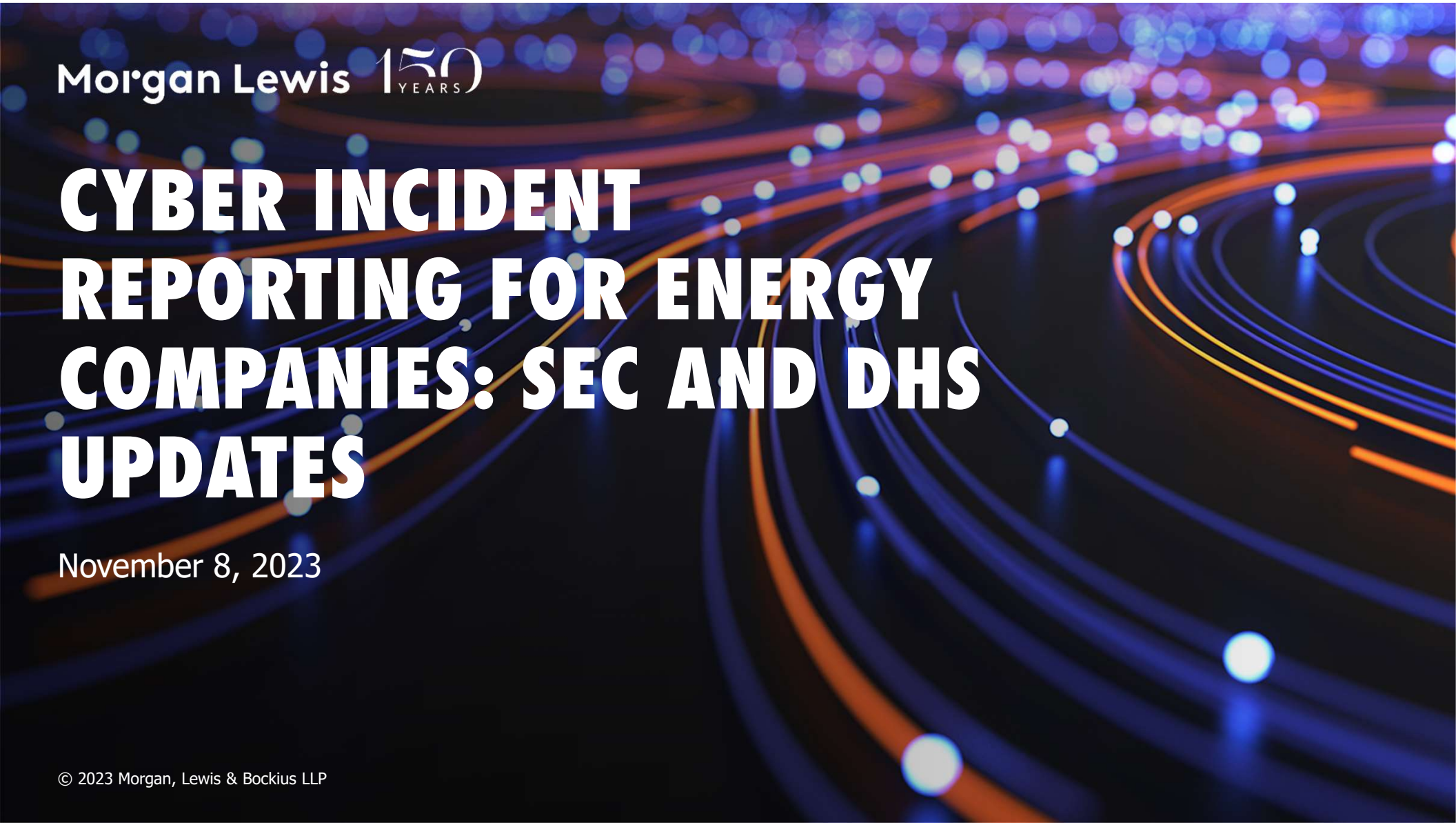


Presenters

J. Daniel Skees

Celia A. Soehner

Arjun Prasad Ramadevanahalli

Agenda

- New SEC Rules on Mandatory Cybersecurity Disclosures
- Updates on Implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022
- Efforts on the Harmonization of Cyber Incident Reporting Requirements


New SEC Rules on Cybersecurity Disclosures
Morgan Lewis
150 YEARS
Global Public Company Academy

Background of Cybersecurity Rules

- On March 9, 2022, the SEC proposed rules that would expressly mandate cybersecurity disclosures by public companies ("Proposed Rules")
- Policy was grounded in –
  - SEC's concern as to the **increasing prevalence** of cyber incidents;
  - Companies' ever-rising **reliance on information systems**
  - Extensive, and potentially material, **costs to companies** from both cyber protection and cyber incidents, which in term can impact stock prices and stockholder value
  - SEC's view that cybersecurity is a **critical governance-related** issue for boards and investors, with various stakeholders demanding more information on cybersecurity risk management, strategy and governance practices

SEC's View on Importance of These Rules

"Whether and **how a registrant is managing cybersecurity risks** could impact an investor's return on investment and would be decision-useful information in an investor's investment or considerations."

"Investors would benefit **from more timely and consistent disclosure** about material cybersecurity incidents" and "from **greater availability and comparability of disclosure** by public companies across industries regarding their cybersecurity risk management, strategy and governance practices."

Final SEC Rules

Final Cybersecurity Rules

- On July 26, 2023, the SEC adopted final rules and amendments for mandating disclosure regarding cybersecurity risk management, strategy, governance, and incident reporting (the "Final Rules").
- The Final Rules are effective September 5, 2023, and require **real-time disclosure** of material cybersecurity incidents, as well as **ongoing disclosure** regarding a company's cybersecurity risk management, strategy, and governance, as well as board of directors' cybersecurity expertise.

Cybersecurity Disclosure – Overview

In summary, the Final Rules:

- **Add a new Item 1.05 to Form 8-K requiring disclosure of material cybersecurity incidents; and**
- **Require periodic disclosure regarding cybersecurity matters (through revisions to Form 10-K and the addition of a new Item 106 to Regulation S-K).**
  - **Note**: In a departure from the Proposed Rules, the SEC did not adopt provisions that would have required disclosure of individual board members' cybersecurity expertise, aggregation of immaterial cybersecurity incidents for materiality analyses, or updates on previously-reported material cybersecurity incidents in periodic or annual reports.

Cybersecurity Rules – Form 8-K

New Item 1.05 to Form 8-K

Requires disclosure within four business days after a company determines that it has experienced a material cybersecurity event.

➡ Meant to address concern that material cybersecurity incidents are underreported

Disclosure would need to include (i) material aspects of the nature, scope and timing of the incident and (ii) the material impact (or likely material impact) on the company, including its financial condition and results of operations

The disclosure would be triggered on the date on which a registrant determines a cybersecurity incident is material, rather than the date of discovery of the incident.

➡ Acknowledges that materiality determination will not always coincide with discovery date

Cybersecurity Rules – Form 8-K – Triggers

Triggers for Reporting

- Within four business days of the determination that the company has experienced a material cybersecurity incident (rather than the date of the incident or discovery of the incident)
  - In other words, the triggering date for the Form 8-K filing is the date that the company concludes that a cybersecurity incident is material.
- **Note**: While the Final Rules do not impose a deadline for determining materiality, they do require that, following the discovery of an incident, companies determine the materiality of the incident through an informed and deliberative process "without unreasonable delay."
- **Note**: There is an extremely limited exception to the four-day deadline: disclosure may be delayed if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

Cybersecurity Rules – Form 8-K – More Detail

- Examples of incidents that could trigger the obligation:
  - The compromise of confidentiality, integrity, or availability of data or a network;
  - An impact on operational technology systems;
  - Harm to a company's reputation, customer or vendor relationships, or competitiveness;
  - The theft, unavailability, or authorization of sensitive business information; extortion-related threats to release stolen information; and
  - Ransomware attacks.
- The SEC stressed that the new Item 1.05 requires disclosure primarily on the impacts of a material cybersecurity incident, rather than details regarding the incident itself
- Unlike the Proposed Rules, the Final Rules do not affirmatively require disclosure of technical information about an incident's remediation status or potential system vulnerabilities

Cybersecurity Rules – Form 8-K – Technicalities

- The Final Rules direct companies to include in their initial Item 1.05 Form 8-K filing a statement identifying any information required under Item 1.05 that is not yet determined or that is unavailable at the time of the required filing.
  - Within four days of such missing information becoming available, the company should then file a Form 8-K amendment containing such information.
- Disclosure under the new Item 1.05 will be deemed to be filed rather than furnished with the SEC for purposes of liability under Section 18 of the Exchange Act, and the Final Rules include amendments to Rules 13a-11(c) and 15d-11(c) under the Exchange Act to include Item 1.05 in the list of Form 8-K items that are eligible for a limited safe harbor liability under Section 10(b) or Rule 10b-5 under the Exchange Act.
- The Final Rules also amend Form S-3 "safe harbor" provisions to provide that a failure to file an Item 1.05 Form 8-K will not result in loss of Form S-3 eligibility.

Materiality Assessment and Reasonable Investor Test

- A key implication of the Final Rules is that companies should have processes in place to not only manage the risk of cybersecurity events, but to also assess the materiality of such events in short order upon occurrence.
- In the Final Rules, the SEC referenced the standard definition of materiality that courts apply in federal securities law cases –
  - Information is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if a disclosure would "significantly alter[] the 'total mix' of information made available" to investors. *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988).
  - A materiality analysis should include both quantitative and qualitative assessments.

SEC's Cybersecurity Reporting Requirements: Materiality Assessment and Reasonable Investor Test (Continued)

- The Final Rules provide nonexhaustive examples of factors that the SEC would expect companies to consider in making materiality assessments:
  - Reputational harm;
  - Data theft;
  - Asset, intellectual property, or business value loss;
  - Harm to customer or vendor relationships;
  - Competitive harm; and
  - The possibility of litigation or regulatory investigation or actions.
- Additionally, the Final Rules confirm that "most companies' materiality analyses will include consideration of the financial impact of a cybersecurity incident."

SEC's Cybersecurity Governance Disclosures

- The Final Rules require that a company in its Form 10-K:
  - Describe its processes, if any, for the identification and management of risks from cybersecurity threats, including:
    - whether such cybersecurity processes have been integrated into the company's overall risk management system or processes;
    - whether the company engages third-party assessors, consultants, or auditors in connection with any such processes; and
    - whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service providers.

SEC's Cybersecurity Governance Disclosures (cont.)

Periodic Reporting of Cybersecurity Matters under New Item 106 of Regulation S-K

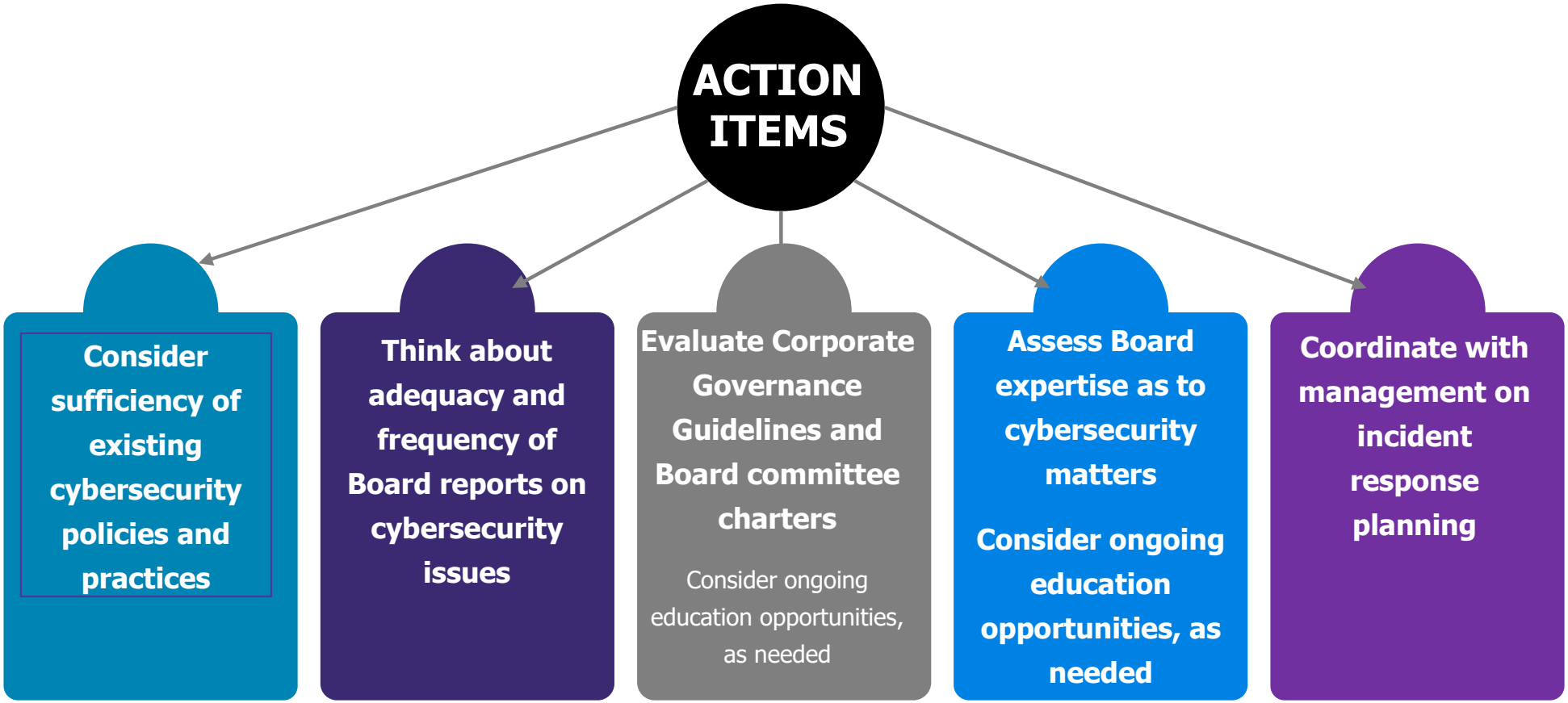
- The Final Rules require that a company in its Form 10-K:
  - Provide disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing material cybersecurity risk and implementing the company's cybersecurity policies, procedures, and strategies, including:
    - whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members (in such detail as necessary to fully describe the nature of the expertise);
    - the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
    - whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

SEC's Cybersecurity Reporting Requirements: Compliance Dates

The Final Rules become effective September 5, 2023.

- With respect to compliance with the incident disclosure requirements in Item 1.05 of Form 8-K, companies must begin complying on December 18, 2023.
- With respect to Item 106 of Regulation S-K, companies must provide such disclosures beginning with Annual Reports on Forms 10-K for fiscal years ending on or after December 15, 2023.
  - **Note**: For calendar year-end issuers, this means that such disclosure will be required for Form 10-Ks filed in early 2024.

Considerations: Cybersecurity Rules




Cyber Incident Reporting for Critical Infrastructure Act of 2022
Morgan Lewis
150 YEARS
Global Public Company Academy

Long Awaited Federal Law for Cyber Incident Reporting

- In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), Public Law 117–103, Div. Y
- Requires owners and operators of critical infrastructure to report cyber incidents and ransom payments to CISA
  - CISA is tasked with developing regulations to fill in the gaps.
- Reporting is mandatory and subject to enforcement
  - 72-hour deadline for covered cyber incidents; 24-hour deadline for ransom payment
  - CIRCIA gives CISA subpoena power and other enforcement tools

Open Implementation Issues

- 2022 CISA RFI highlighted key issues:
  - Applicability: Gating definitions ("Covered entity", "covered cyber incident", "reasonable belief")
  - Timing: Determining "when the clock starts"
  - Harmonization: How should CISA rules stack up with other regulatory requirements?
  - Third Party Implications: Supply chain compromise / third party suppliers
  - Enforcement and Liability: How will broad subpoena power be used?

Applicability

- CISA must complete rulemaking activities to define scope of requirements
- "Covered entity"
  - An entity in one of the 16 critical infrastructure sectors defined in PPD-21
- "Covered cyber incident"
  - Statute includes threshold criteria (e.g., loss of availability of information system or network, impact on the safety and resiliency of operational systems and processes)

Reporting Timelines

Covered cyber incident

- "A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity ***reasonably believes*** that the covered cyber incident has occurred."

Ransomware payment

- "A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours ***after the ransom payment has been made***."

Protections for Covered Entities

- Liability protections
  - "No cause of action shall lie or be maintained in any court . . . for the submission of a report . . . that is submitted *in conformance with this subtitle*"
- Confidentiality of submitted information
  - FOIA-exempt
  - Considered commercial, financial, and proprietary information of covered entity when so designated
  - No waiver of any privilege or legal protection
  - Not subject to any *ex parte* rule of any federal agency or judicial doctrine

Implications for Third Party Providers

- Reportable incidents must include unauthorized access or operational disruption due to loss of service from:
  - Cloud service provider;
  - Managed service provider;
  - Other third-party data hosting provider; or
  - Supply chain compromise.
- Third party submitter
  - CIRCIA allows a covered entity to use a third party, such as an incident response company, insurance provider, service provider, or law firm, to submit required reports.

Enforcement

- CIRCIA grants CISA broad enforcement authority
- Subpoena power
  - If unable to obtain information directly from covered entity within 72 hours, Director may issue a subpoena to "gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred"
- Civil action
  - Director can refer to Attorney General to bring civil action in US District Court
- Referral for regulatory enforcement
  - CISA can refer to other federal regulators if it determines that information gained in response to subpoena "may constitute grounds for a regulatory enforcement action or criminal prosecution"

Related Risks and Legal Liability

- Heightened scrutiny from other regulators
- Private lawsuits
- Reputational harm
- Financial ripple effects
- Compliance enforcement exposure

Next Steps

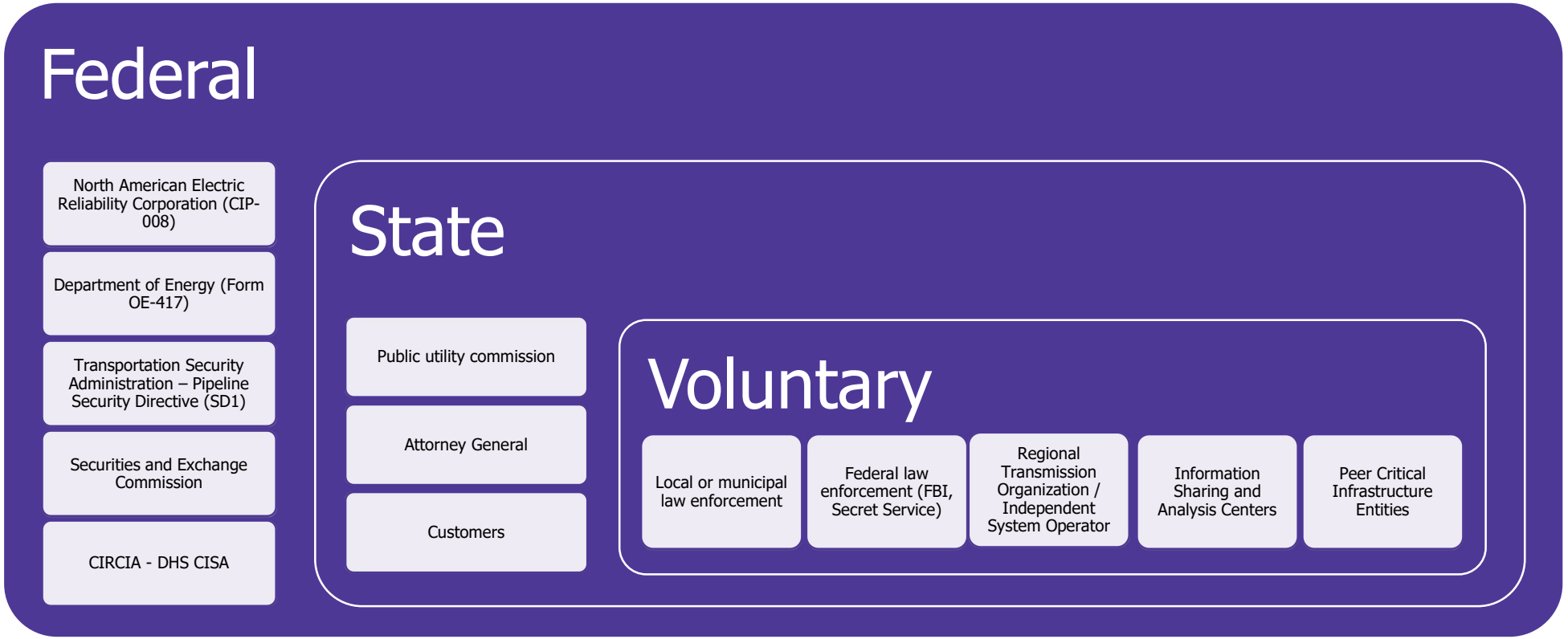
- CISA formalizing rulemaking
  - CISA completed "listening sessions" to solicit feedback from public and stakeholders.
- Implementation
  - Notice of Proposed Rulemaking (NPRM) due by March 2024, but reportedly ahead of schedule.
  - Final rule must be issued within 18 months after publication of NPRM.


Harmonization of Cyber Incident Reporting Requirements
Morgan Lewis
150 YEARS
Global Public Company Academy

Implementation Challenges

- Energy industry entities are already subject to multiple overlapping cyber incident reporting requirements.
- Disparate requirements driven by different regulatory/policy objectives
  - National security
  - Public safety
  - Consumer protection
  - Market transparency and shareholder protection

Stacking Incident Reporting Requirements



DHS Report on Harmonization

- In CIRCIA, Congress established a Cyber Incident Reporting Council (CIRC) to coordinate, deconflict, and harmonize federal incident reporting requirements
  - CIRC comprehensively assessed 52 in-effect or proposed federal cyber incident reporting requirements
- Results
  - 45 requirements are currently in effect across 22 agencies
  - Significant duplication for certain entities that is magnified by the application of cross-sector regulatory requirements and voluntary reporting
  - Divergent timelines and triggers for reporting cyber incidents also present a significant challenge

CIRC Recommendations to Streamline Reporting

1. Adopt a model definition of a reportable cyber incident wherever practicable.
2. Adopt model cyber incident reporting timelines and triggers wherever practicable
3. Agencies should consider allowing delays to notifications
4. Adopt a model reporting form for cyber incident reports wherever practicable
5. Streamline receipt and sharing of cyber incident reports and cyber incident information.
6. Reporting requirements should allow for updates and supplemental reports.
7. Adopt common terminology regarding cyber incident reporting wherever practicable.
8. Improve processes for engaging with reporting entities following the initial report of a cyber incident.


Future of Cyber Incident Reporting
Morgan Lewis
150 YEARS
Global Public Company Academy

Artificial Intelligence (AI)

- Entities routinely implement robust monitoring and alerting tools, but struggle to screen out the noise.
  - Vast quantities of data, low-level attacks, and "false positives" create challenges for deriving meaningful and timely insights on potential cyber incidents.
  - Historical reliance on human analysts and SOC coordination to initiate incident response activities.
- Some solutions already leverage monitoring and machine learning to streamline security operations.
  - SIEM
  - SOAR
- Greater integration of AI in triage and incident response activities is likely.
  - Greater efficiency
  - Identifying abnormalities and automated responses

Executive Order on AI

- October 30, 2023 Executive Order
  - NIST to develop AI standards to ensure systems are "safe, secure, and trustworthy"
  - DHS to implement them in critical infrastructure sectors
  - DHS to establish an AI Safety and Security Board
  - DHS and DOE to assess AI threats to critical infrastructure sectors
    - "an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks, and shall consider ways to mitigate these vulnerabilities."
- Takeaways: Likely to introduce caution on the use of AI in critical infrastructure, particularly in ways that could result in harm to that infrastructure due to misuse or unpredictability


Questions
Morgan Lewis
150 YEARS
Global Public Company Academy

Biography

J. Daniel Skees
Washington, D.C.
+1.202.739.5834
daniel.skees@morganlewis.com

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, utility financing, electric markets and trading issues, reliability standards development and compliance, including cybersecurity requirements, administrative litigation, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit. He currently serves as a deputy practice group leader for the firm's energy and project development practice.

Biography

Celia A. Soehner
Pittsburgh, PA
+1.412.560.7441
celia.soehner@morganlewis.com

Celia A. Soehner is co-leader of the firm's capital markets and public companies practice and co-leads the firm's ESG and sustainability advisory practice. She focuses her practice on counseling public companies and their boards with respect to corporate governance, federal securities, stock exchange, shareholder engagement, ESG, and executive compensation matters. Drawing on her previous tenure as an attorney-advisor with the US Securities and Exchange Commission (SEC) in the Division of Corporation Finance, Celia has experience with securities disclosure issues that impact public companies' ongoing reporting obligations and proxy-related matters that impact public companies and their officers and directors. She also advises companies in connection with public capital raising transactions, including through IPOs, secondary offerings, and debt offerings.

Biography

Arjun Prasad Ramadevanahalli
Washington, D.C.
+1.202.739.5913
arjun.ramadevanahalli@morganlewis.com

Arjun Prasad Ramadevanahalli represents electric power, natural gas, and oil industry participants in regulatory and transactional matters. He assists clients on issues regarding wholesale markets, utility transactions, rate matters, and enforcement proceedings before the Federal Energy Regulatory Commission (FERC), and on cybersecurity matters in the energy industry. Arjun regularly advises utilities and other industry participants on North American Electric Reliability Corporation (NERC) reliability standards enforcement and compliance matters, including cybersecurity compliance and controls under the Critical Infrastructure Protection (CIP) suite of standards. Arjun counsels pipeline owners and operators on cybersecurity compliance before the Transportation Security Administration (TSA).

THANK YOU

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Shenzhen
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis 150 YEARS