Cybersecurity Incident Disclosure

Christopher Holt
Associate General Counsel

Risk Management Committee
January 23, 2024

Cyber Incident Disclosure

What is the objective of the PS/IC?

PJM is seeking to have Members provide PJM with notice of a successful breach of the Member's cybersecurity. The objective is so that PJM can address any credit risk concerns and take any appropriate steps to protect PJM and Member confidential data and systems.

What is not being requested?

PJM is not looking to prescribe any technical requirements or technical solutions.

What is the basis for this request?

- The promulgation of recent SEC rule that requires all SEC-registered companies and foreign registrants to provide notice of a material cybersecurity incident within four business days **(see appendix)**
- Economic activity more dependent on electronic systems
- Increase in threat actors
- Increase in cybersecurity incidents
- Increase in costs and consequences of cyber incidents

Attack on PJM Member and compromise Member IT/Security:

- ••Potential Material Adverse Event (MAE) trigger?
- ••Potential effects on PJM IT/Security systems?
- ••Potential impacts on transmission grid?
- ••Potential effects and compromise of PJM and Member data?
- ••Potential impacts on other Members?

Existing Manual 13 Obligations

Manual 13	• Constant cybersecurity monitoring to ensure PJM cyber assets maintain reliable operations.
	• If credible cyberthreat, PJM alerts its respective incident response teams to investigate and address the cyberthreat.
	• PJM notifies members of impacted systems and necessary actions via the All-Call.
	• PJM also has obligations regarding protection of confidential information and communication regarding release of confidential information.

Additional PJM Reporting

PJM Reporting

- PJM works closely with Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. PJM has access to federally protected confidential information.
- PJM is a member of the NERC EISAC (Electricity Information Sharing and Analysis Center) and shares certain cyber information in accordance with the terms of its membership, which is operated in accordance with federal law by NERC as the ERO and subject to certain disclosure restrictions.
- PJM also has reporting obligations to the Department of Energy pursuant to DOE 417.

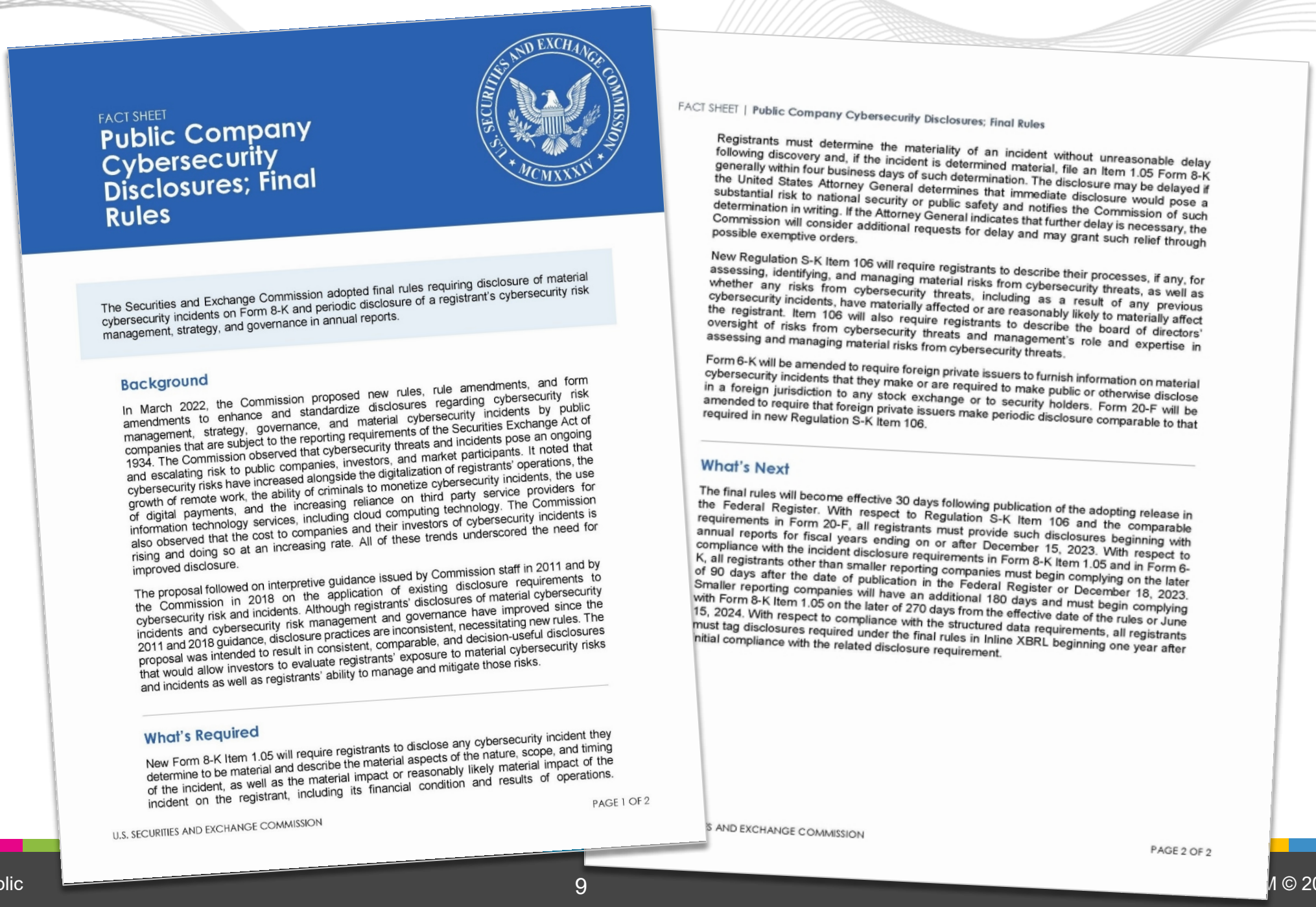
Next Steps

PJM is seeking that (i) Members subject to the SEC rule to provide notice and (ii) non-SEC-regulated companies do the same.

PJM could request information under existing authority but recognizes that the provision of such notice may need to include third-party asset/energy managers who have access to the PJM system and address limitations that Members may have similar federally imposed confidentiality obligations.

PJM is seeking input thru the PS/IC to define workable reporting rules to address Member credit risk, confidentiality concerns and potential Member-related cyber risk.

Appendix



FACT SHEET

Public Company Cybersecurity Disclosures; Final Rules

The Securities and Exchange Commission adopted final rules requiring disclosure of material cybersecurity incidents on Form 8-K and periodic disclosure of a registrant's cybersecurity risk management, strategy, and governance in annual reports.

Background

In March 2022, the Commission proposed new rules, rule amendments, and form amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. The Commission observed that cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants. It noted that cybersecurity risks have increased alongside the digitalization of registrants' operations, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising and doing so at an increasing rate. All of these trends underscored the need for improved disclosure.

The proposal followed on interpretive guidance issued by Commission staff in 2011 and by the Commission in 2018 on the application of existing disclosure requirements to cybersecurity risk and incidents. Although registrants' disclosures of material cybersecurity incidents and cybersecurity risk management and governance have improved since the 2011 and 2018 guidance, disclosure practices are inconsistent, necessitating new rules. The proposal was intended to result in consistent, comparable, and decision-useful disclosures that would allow investors to evaluate registrants' exposure to material cybersecurity risks and incidents as well as registrants' ability to manage and mitigate those risks.

What's Required

New Form 8-K Item 1.05 will require registrants to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.

PAGE 1 OF 2

U.S. SECURITIES AND EXCHANGE COMMISSION

Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of such determination. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. If the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through possible exemptive orders.

New Regulation S-K Item 106 will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant. Item 106 will also require registrants to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Form 6-K will be amended to require foreign private issuers to furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction to any stock exchange or to security holders. Form 20-F will be amended to require that foreign private issuers make periodic disclosure comparable to that required in new Regulation S-K Item 106.

What's Next

The final rules will become effective 30 days following publication of the adopting release in the Federal Register. With respect to Regulation S-K Item 106 and the comparable requirements in Form 20-F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Form 8-K Item 1.05 and in Form 6-K, all registrants other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024. With respect to compliance with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

S AND EXCHANGE COMMISSION

PAGE 2 OF 2

Contact

Facilitator:
Thomas Zadlo,
Thomas.Zadlo@pjm.com

Secretary:
Emmy Messina, Emmy.Messina@pjm.com

SME/Presenter:
Christopher Holt, Christopher.Holt@pjm.com

Cybersecurity Incident Disclosure

Member Hotline

(610) 666-8980

(866) 400-8980

custsvc@pjm.com

PROTECT THE POWER GRID

THINK BEFORE YOU CLICK!

pjm

Be alert to malicious phishing emails.

Report suspicious email activity to PJM.

(610) 666-2244 / it_ops_ctr_shift@pjm.com