WHERE FROM HERE?

NAVIGATING THE NEW MARKET

A resource for insights, information, benchmarking and conversation

orrick

Panelists

Carolyn Frantz
Co-Head, Public Companies & ESG Practice
Orrick

J.T. Ho
Co-Head, Public Companies & ESG Practice
Orrick

Mike Pressman
Assistant General Counsel
Microsoft

Aravind Swaminathan
Partner, Cyber, Privacy & Data Innovation Group
Orrick

THE SEC'S PROPOSED RULES FOR CYBERSECURITY AND CLIMATE: IMPLICATIONS FOR ESG DISCLOSURE AND INTERNAL CONTROLS

April 19, 2022

orrick

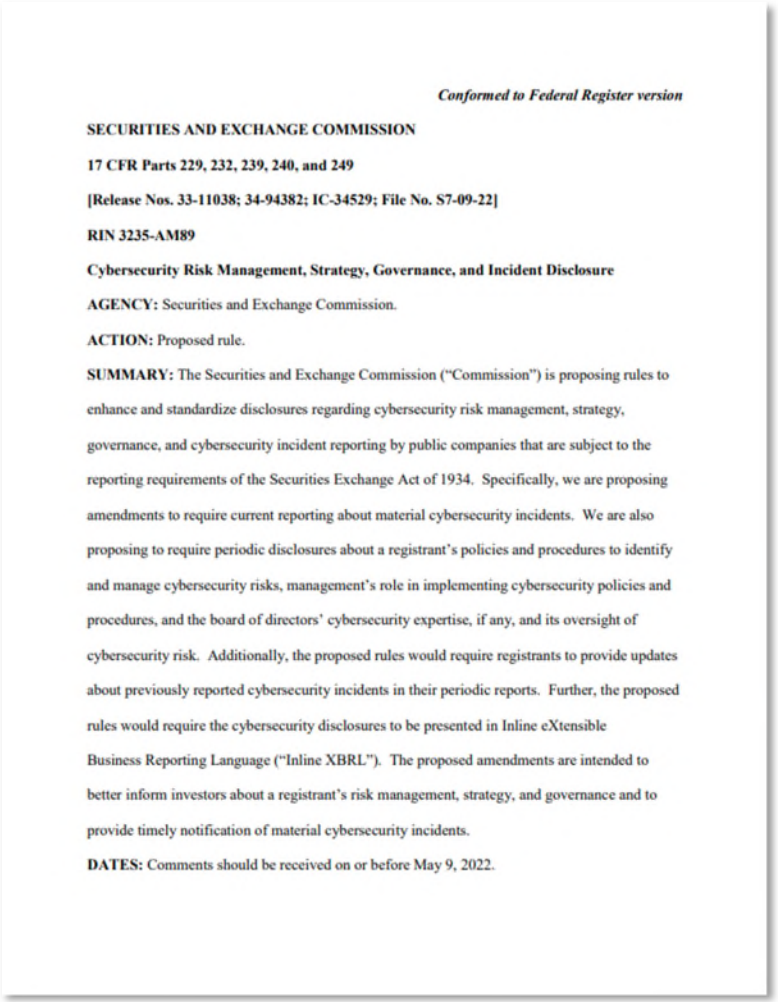
Welcome and Agenda

- Overview of SEC Proposed Disclosure Rules
  - Cybersecurity
  - Climate
  - Expected Human Capital Management
- Themes from SEC Rulemaking
- Takeaways
  - Board Governance
  - Enterprise Risk Management and Internal Audit
  - Disclosure Considerations
  - Implications for Talent
  - Implications for Programs

Proposed Cybersecurity Rules: Key Provisions

The proposed rules require publicly traded companies, including FPIs, to disclose:

- Material cybersecurity incidents on Form 8-K/6-K:
  - Timing tied to a company's determination that the incident is material
  - Materiality determination to be made as soon as "reasonably practicable"
  - Includes reporting of certain third-party incidents
  - No law enforcement exception
- Updates to incidents, and certain aggregated incidents, in 10-Qs/10-Ks/20-Fs
- In the proxy statement (or 20-F for FPIs):
  - policies and procedures to identify and manage cybersecurity risks;
  - the role of cybersecurity in strategy, financial planning, and capital allocation;
  - the process of board oversight and any directors with expertise;
  - management's role, expertise, and processes



Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is proposing rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents. We are also proposing to require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk. Additionally, the proposed rules would require registrants to provide updates about previously reported cybersecurity incidents in their periodic reports. Further, the proposed rules would require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL"). The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.

DATES: Comments should be received on or before May 9, 2022.

Proposed Cybersecurity Rules: Action Items

Companies should be considering:

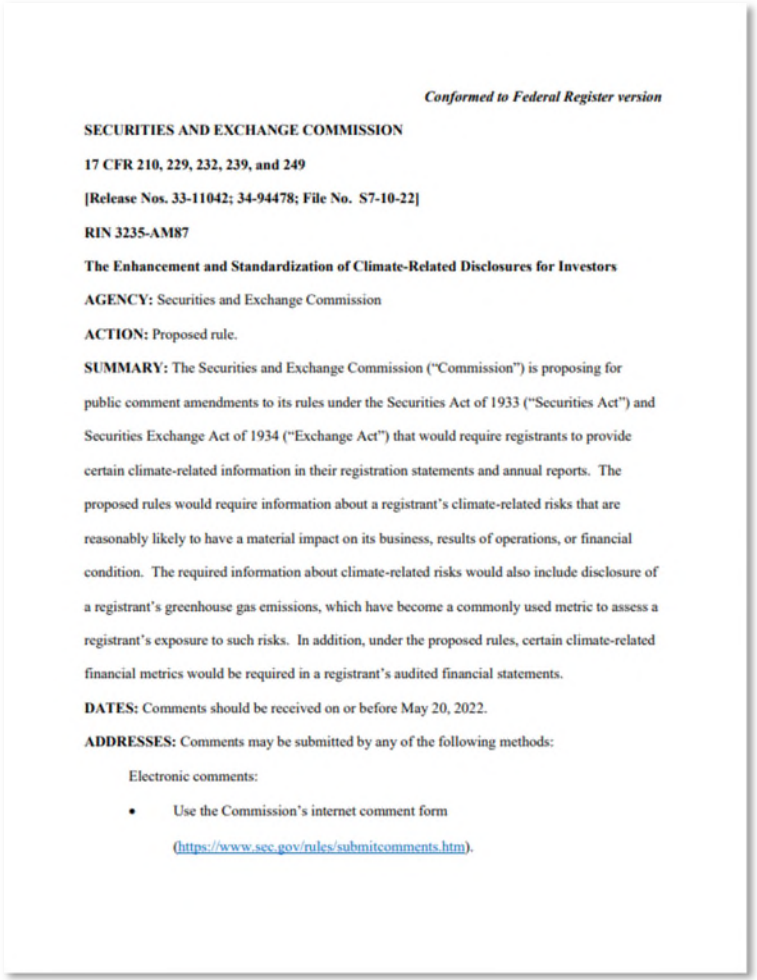
- Updating incident response framework and process for assessing severity of incidents and escalation
- Incorporating Disclosure Committee into incident response process
- Documenting Company processes for assessing materiality, and important determinations
- Integrating SEC disclosures with other incident communications/notification methods, including preparing for earlier response
- Updating vendor contracts to support enhanced information gathering

Proposed Climate Change Rules: Key Provisions

The proposed rules require publicly traded companies (including FPIs) to disclose in registration statements and annual reports:

- Scope 1 and Scope 2 greenhouse gas ("GHG") emissions and carbon intensity
  - Scope 3 GHG emissions and carbon intensity need to be disclosed if material, or if a company has set a Scope 3 GHG emissions reduction target or goal.
- Material risks related to climate change, including whether such risks are likely to manifest in the short, medium or long-term.
- Climate-related costs, capital expenditures and reserves if those exceed a certain threshold in the financial notes.
- Board and management oversight of climate-related risks, processes for identifying, assessing, and managing such risks, and integration with the company's overall risk management function and processes.
- Information regarding publicly identified climate-related goals, including any interim goals, the time horizon for achievement, how the company intends to achieve these goals, and progress towards these goals.

In addition, companies must obtain third-party assurance of Scope 1 and 2 GHG emissions data by certain deadlines.



Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR 210, 229, 232, 239, and 249

[Release Nos. 33-11042; 34-94478; File No. S7-10-22]

RIN 3235-AM87

The Enhancement and Standardization of Climate-Related Disclosures for Investors

AGENCY: Securities and Exchange Commission

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is proposing for public comment amendments to its rules under the Securities Act of 1933 ("Securities Act") and Securities Exchange Act of 1934 ("Exchange Act") that would require registrants to provide certain climate-related information in their registration statements and annual reports. The proposed rules would require information about a registrant's climate-related risks that are reasonably likely to have a material impact on its business, results of operations, or financial condition. The required information about climate-related risks would also include disclosure of a registrant's greenhouse gas emissions, which have become a commonly used metric to assess a registrant's exposure to such risks. In addition, under the proposed rules, certain climate-related financial metrics would be required in a registrant's audited financial statements.

DATES: Comments should be received on or before May 20, 2022.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic comments:

- Use the Commission's internet comment form (https://www.sec.gov/rules/submitcomments.htm).

Proposed Climate Change Rules: Action Items

Companies should be considering:

- Reevaluating or developing reporting structures to collect and report on GHG emissions and intensity
- Revisiting existing disclosure controls and procedures, including the structure of the disclosure committee
- Reevaluating or identifying potential attestation providers, and making sure that such providers qualify under the proposed rules
- Refining or developing formal climate risk oversight processes at the board and management level
- Revisiting how the company aims to achieve its climate goals (if any) and how progress is being tracked, and whether adjustments need to be made

Prediction: Proposed Human Capital Management Rules

- The current human capital management ("HCM") disclosure rule requires companies describe the company's human capital resources, including the number of persons employed by the company, and any human capital measures or objectives that the company focuses on in managing the business, the 10-K.
- Studies have shown little disclosure of metrics beyond employee headcount, which is strictly required by the rule. A growing number of companies are also disclosing EEO-1 data, following shareholder requests.
- Based on remarks from the SEC, the proposed HCM rules are likely to be much more prescriptive, and may include "**metrics, such as workforce turnover, skills and development training, compensation, benefits, workforce demographics including diversity, and health and safety**."
- The proposed cybersecurity and climate change rules suggest that the proposed HCM rules could also require disclosing human capital risks and oversight of risk at both the board and management level. SEC's enforcement actions also suggest a possible focus on oversight of culture.
- The current rules do not apply to foreign private issuers or smaller reporting companies – will the SEC include them in the new rule?

SEC Rulemaking: Themes and Trends

"A registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident"

"[Disclosure required] about the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic"

"[A]nother proposed item would require disclosure about the processes by which the responsible managers or management committees are informed about and monitor climate-related risks"

"Quantitative greenhouse gas ("GHG") emissions data can enable investors to assess a registrant's exposure to climate-related risks, including regulatory, technological, and market risks driven by a transition to a lower-GHG intensive economy."

- Increased SEC focus on **process disclosure**
- SEC increasingly seeking disclosure of **specific uniform data**, regardless of whether material to the issuer
- SEC seeking detailed **board governance disclosures** – personnel, processes, and views
- SEC seeking detailed **disclosure about management-level governance** – personnel, processes, and views
- SEC focused on **risk management programs** and related disclosures

Board Governance

Questions to Consider

Does your director skills matrix and director succession strategy reflect the key ESG and cybersecurity risks identified by enterprise risk management?

Do your board and committee calendars reflect key risks?

Do your board and committee materials and minutes cover the SEC's areas of focus for both cyber and climate: "Whether and how the board or board committee considers … risks as part of its **business strategy**, **risk management**, and **financial oversight**."

Is your board assessment process adequate to evaluate governance and skills related to ESG and cybersecurity?

Does your board need education about these evolving issues?

Sidebar: Litigation Risks

"Airplane safety was not a regular set agenda item or topic at Board meetings. Audit Committee and ERV materials reveal that airplane safety risks were not discussed."

"None of Boeing's Board committees were specifically tasked with overseeing airplane safety, and every committee charter was silent as to airplane safety…This stood in contrast to many other companies in the aviation space whose business relies on the safety and flightworthiness of airplanes."

Boeing MAX, Del. Chancery (2021)

Enterprise Risk Management and Internal Audit

CLIMATE: *"The proposed rules would require registrants to describe their processes for identifying, assessing, and managing climate-related risks. This includes disclosure on how registrants assess materiality, whether they consider likely future regulatory actions, how they prioritize, mitigate, or adapt to climate-related risks, and overall how climate-related factors are integrated into the registrants' **risk management systems or processes**."*

CLIMATE: *"How any climate-related risks identified by the registrant have had or are likely to have a material impact on its business and consolidated financial statements, which may manifest over the **short-, medium-, or long-term**."*

CYBER: *"We are proposing Item 106(b) of Regulation S-K to require registrants to provide more consistent and informative disclosure regarding their **cybersecurity risk management and strategy**."*

Questions to Consider

Is your Enterprise Risk Management process consistent with and informed by your ESG priority assessment and your cybersecurity risk assessment?

Do your ESG priority assessment and cybersecurity risk assessment processes follow best practices learned from your ERM program?

Is your risk management program prepared to categorize risks by short-, medium-, and long-term impact?

Should you consider greater full board review of ERM?

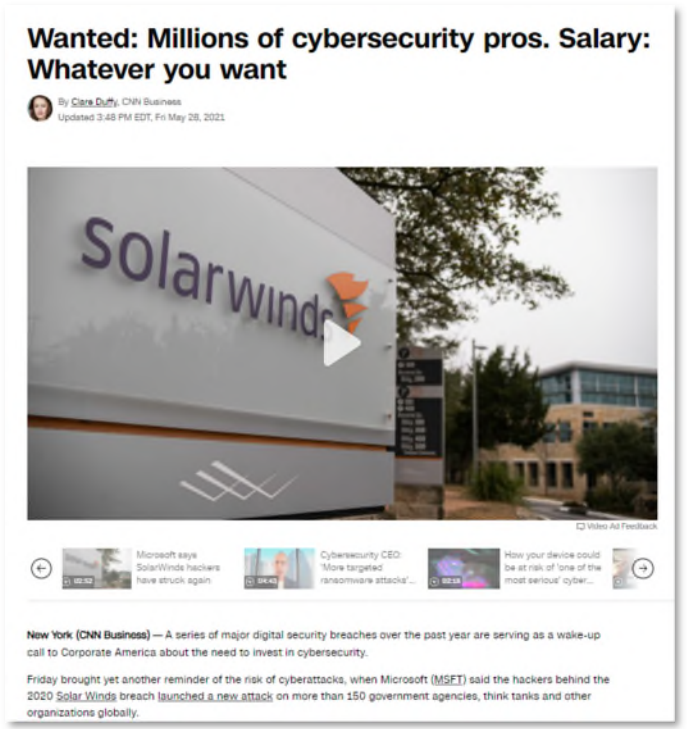
Does your internal audit program have the resourcing and mandate to evaluate climate-related projects and initiatives?

Disclosure Considerations

Companies should consider:

- Evaluating whether your **ESG/CSR report** ties your reporting to the Company's long-term financial success
- Creating a **calendar of required and voluntary disclosures**, and evaluating whether certain disclosures should be coordinated – particularly aligning timing of ESG report and 10-K to enhance consistency
- Creating a formal system for **evaluating consistency** across SEC disclosures and voluntary disclosures (ESG and CSR reports, as well as responses to ESG and other ratings surveys)
- Creating a responsibility chart for **legal review of disclosures**, ensuring the right in-house and outside counsel are involved in review of the appropriate questions
- Whether **additional individuals** should be added to Disclosure Committees to address these new disclosures
- Practically, whether your Disclosure Committee has the time to handle all of this, or if it would be better to create a **subcommittee** or rely on the leader of an **operational office** responsible for ESG disclosures
- Whether **sub-certifications** should be required for voluntary disclosures, or additional documentation required for non-disclosure of cyber incidents
- Having a dialogue with the **independent auditor** about their expectations for audit scope and needs; identifying additional third-party assurance providers

Implications for Talent



Wanted: Millions of cybersecurity pros. Salary: Whatever you want

By Clare Duffy, CNN Business
Updated 3:48 PM EDT, Fri May 28, 2021

Microsoft says SolarWinds hackers have struck again

Cybersecurity CEO: 'More targeted ransomware attacks'...

How your device could be at risk of 'one of the most serious' cyber...

New York (CNN Business) — A series of major digital security breaches over the past year are serving as a wake-up call to Corporate America about the need to invest in cybersecurity.

Friday brought yet another reminder of the risk of cyberattacks, when Microsoft (MSFT) said the hackers behind the 2020 Solar Winds breach launched a new attack on more than 150 government agencies, think tanks and other organizations globally.

Average tenure of a CISO?
26 months.

Recruiting and retention for positions relevant to the SEC's priority areas will be key.

Issuers have long struggled with these issues with cybersecurity professionals. Required reporting about management changes will make retention even more important to many issuers.

Job listings for ESG program managers, counsel, and data analysts have recently skyrocketed (see just one page from Amazon's "ESG" job listings, right).

ESG Strategist / Program Manager — Posted March 17, 2022 (Updated about 1 month ago)
GBR, London | Job ID: 1987226
Basic qualifications:
- 5+ years of experience in ESG investment or with an environmental or human rights NGO.
- 5+ years of experience managing, analyzing and communicating results to senior management.

...Read more

ESG Strategist / Program Manager — Posted October 22, 2021 (Updated 2 months ago)
USA, VA, Arlington | Job ID: 1785113
Basic qualifications:
- 5+ years of experience in program or project management
- Experience using data and metrics to drive improvements
- Experience owning program strategy, end to end delivery, and communicating results to senior leadership

...Read more

Worldwide Lead, ESG Reporting , WW Sustainabiilty — Posted March 25, 2022 (Updated 19 days ago)
USA, CA, San Francisco | Job ID: 1996179
Basic qualifications:
- Minimum 10+ years of experience working in sustainability, ESG, legal or public policy fields.
- Proven track record leading global projects with high levels of complexity.
- Strong written and oral communicator.

...Read more

Head of Worldwide ESG Reporting & Disclosures, WW Sustainabiilty — Posted March 4, 2022 (Updated 19 days ago)
USA, VA, Arlington | Job ID: 1969206
Basic qualifications:
- 15+ years of experience working in sustainability, ESG, legal or public policy fields.
- 15+ years experience building teams and managing people.
- 15+ years experience managing vendors.
- 15+ years experience allocating and managing budgets

...Read more

Corporate Counsel, Sustainability — Posted March 8, 2022 (Updated about 1 month ago)
USA, VA, Arlington | Job ID: 1974237
Basic qualifications:
- J.D. degree from an accredited law school and active membership in one state bar;
- 5+ years of legal experience as a licensed attorney, with experience in counseling companies on ESG reporting and/or corporate, securities and governance matters; and
- Ability to travel domestically and internationally as needed.

...Read more

Senior Corporate Counsel, WW Sustainability — Posted March 3, 2022

Implications for Programs

- Expect creation of disclosure-ready standardized, generic, programs and policies
- Governance disclosures likely bare-bones at first, filled in over time by SEC comment letters and enforcement
- More caution in climate-related goals, especially Scope 3; some walk-backs
- Most companies determining Scope 3 not material, at least at first
- Cybersecurity incident disclosures may not change much for companies with major cybersecurity risks; may see over-disclosure for others
- Changes in contracting provisions for vendors posing cybersecurity risks
- Massive infrastructure creation around legal support, financial reporting, and ESG program management

WHERE FROM HERE?

NAVIGATING THE NEW MARKET

A resource for insights, information, benchmarking and conversation

orrick