May 10, 2023

A TOUR THROUGH RECENT CYBERSECURITY DEVELOPMENTS

Aaron Charfoos
Paul Hastings LLP

Jeremy Berkowitz
Paul Hastings LLP

Daniel Sutherland
Meta

Privacy+ Security Forum

Speakers

Aaron Charfoos

Partner and Global Chair, Data Privacy and Cybersecurity
Paul Hastings LLP

Daniel Sutherland

Director and Associate General Counsel
Meta

Jeremy Berkowitz

Senior Director, Deputy Chief Privacy Officer
Paul Hastings LLP

- ✓ **THE WHITE HOUSE AND THE BIDEN-HARRIS ADMINISTRATION**
- ✓ **U.S. SECURITIES AND EXCHANGE COMMISSION**
- ✓ **NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES**
- ✓ **WHAT SHOULD COMPANIES BE DOING?**

Privacy+ Security Forum

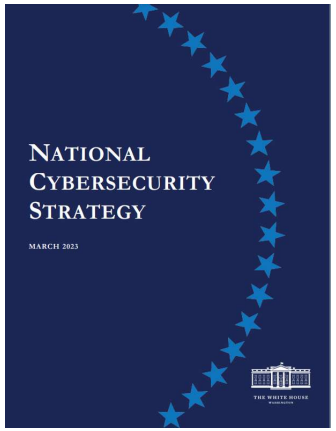
BIDEN-HARRIS NATIONAL CYBERSECURITY STRATEGY

Privacy+ Security Forum

- On **March 3, 2023**, the White House released the **National Cybersecurity Strategy** – a blueprint for a long-term effort by the Biden administration, in cooperation with Congress and the private sector, to address cybersecurity issues

NATIONAL CYBERSECURITY STRATEGY PILLARS

- ✓ **Defend Critical Infrastructure**
- ✓ **Disrupt and Dismantle Threat Actors**
- ✓ **Shape Market Forces to Drive Security and Resilience**
- ✓ **Invest in a Resilient Future**
- ✓ **Forge International Partnerships to Pursue Shared Goals**



SEC PROPOSED RULES AND AMENDMENTS FEBRUARY 2022

Privacy+ Security Forum

- On **February 9, 2022,** the SEC released proposed new rules and amendments addressing cybersecurity risk management and cybersecurity-related disclosures for registered investment advisers, registered investment companies, and funds (including business development companies)
- The SEC comment period will close on **May 22, 2023**

PROPOSED RULE 204-6

Requirements

- ✓ Advisers required to report significant cybersecurity incidents to the SEC promptly, but in no event later than 48 hours
- ✓ Advisers required to submit a report by submitting a new Form ADV-C, which would be confidential

PROPOSED RULES 206(4)-9 & 38A-2

Requirements

- ✓ Policies and procedures
- ✓ Annual reviews and required written reports
- ✓ Fund board oversight
- ✓ Recordkeeping

FORM ADV PART 2A PROPOSED AMENDMENTS

Requirements

- ✓ Advisers required to disclose certain material cybersecurity risks and certain cybersecurity incidents
- ✓ Funds required to disclose any principal cybersecurity risks and significant fund cybersecurity incidents

SEC PROPOSED AMENDMENTS MARCH 2022

Privacy+ Security Forum

- On **March 9, 2022** the SEC released proposed cybersecurity disclosure amendments to its rules for **public companies**
- Comment period reopened late 2022; Date to be finalized is **TBD**

KEY PROPOSED AMENDMENTS

- ✓ **Report "material cybersecurity incidents" to the SEC, using Form 8-K, within 4 days**
- ✓ **Report non-material incidents that, when combined with other incidents, become material "in the aggregate"**
- ✓ **Mandatory disclosure of any material changes on Form 10- Q and Form 10K from the disclosures in the initially filed Item 1.05 8-K**
- ✓ **Provide updates on prior incidents in periodic SEC disclosures**
- ✓ **Provide a description of the company's cybersecurity risk management system**
- ✓ **Describe the Board's oversight of cybersecurity risk**
- ✓ **Disclose the cybersecurity expertise of the Board members**

SEC PROPOSED RULE AND AMENDMENTS MARCH 2023

Privacy+ Security Forum

- On **March 15, 2023,** the SEC issued proposed cybersecurity amendments to current SEC regulations for broker dealers, investment companies, and registered advisors and a new proposed rule addressing cybersecurity requirements for market and covered entities
- Comments are due on **June 5, 2023**

REGULATION S-P PROPOSED AMENDMENTS

Applicability

- ✓ Broker-dealers
- ✓ Investment Companies
- ✓ Registered Investment Advisers

Requirements

- ✓ Customer notification
- ✓ Scope of information under Safeguards Rule and Disposal Rule
- ✓ Recordkeeping
- ✓ Incident response

REGULATION SCI PROPOSED AMENDMENTS

Key Amendments

- ✓ Expanded definition of SCI Entity
- ✓ Strengthening obligations of SCI Entities

PROPOSED RULE 10

Applicability

- ✓ Market Entities
- ✓ Covered Entities

Requirements

- ✓ Policies and procedures
- ✓ Notification and reporting of Significant Cybersecurity Incidents
- ✓ Disclosure of cybersecurity risks and incidents
- ✓ Recordkeeping

PROPOSED NYDFS PART 500 AMENDMENTS

Privacy+ Security Forum

- ✓ Class A Companies: New obligations for large companies. Additional obligations include independent audits, vulnerability assessments, password controls, and monitoring
- ✓ Governance: CISO independence, additional board reporting + expertise, policy approvals, CEO certification, BCDR plans, and tabletop exercises and IRP
- ✓ Risk Assessment: Tailor assessments to the specific organization with annual updates
- ✓ Technology: Proscriptive requirements, including implementing policies and procedures to ensure a complete asset inventory and requirements relating to privileged accounts
- ✓ Notification Obligations: NYDFS must be notified within 72 hours of unauthorized access or deployment of ransomware; within 24 hours for extortion payments + rationale
- ✓ Penalties: Clarifies what constitutes a violation and provides a list of mitigating factors

WHAT SHOULD COMPANIES BE DOING TO PREPARE?

Privacy+ Security Forum

- ✓Review cybersecurity and risk management documents
- ✓Educate the Board and management
- ✓Review incident response plans
- ✓Identify what materiality means to your company

Questions & Contacts

Aaron Charfoos

Partner and Global Chair, Data Privacy and Cybersecurity
Paul Hastings LLP
aaroncharfoos@paulhastings.com

Daniel Sutherland

Director and Associate General Counsel
Meta
dansutherland@meta.com

Jeremy Berkowitz

Senior Director, Deputy Chief Privacy Officer
Paul Hastings LLP
jeremyberkowitz@paulhastings.com