November 8, 2023

UPDATE ON NEW CYBERSECURITY REGULATIONS

Jeremy Berkowitz
Paul Hastings LLP

Spencer Fisher
Cybersecurity & Infrastructure Security Agency

Brandon Pugh
R Street Institute

Johnathan Rudy
Transunion

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Jeremy Berkowitz

Senior Director, Deputy Chief Privacy Officer
Paul Hastings LLP

Spencer Fisher

Chief Counsel, Department of Homeland Security, Cybersecurity & Infrastructure Security Agency

Brandon Pugh

Director, Cybersecurity and Emerging Threats
R Street Institute

Johnathan Rudy

Senior Corporate Counsel, Cybersecurity & Data Protection, Transunion

DISCUSSION OF TOPICS

- ✓ SEC Cybersecurity Incident Response Rules
- ✓ NYDFS Part 500 Amendments
- ✓ CCPA Security Audits and Assessments
- ✓ Artificial Intelligence Executive Order
- ✓ DHS Secure-by-Design Guidance
- ✓ Harmonization of Cyber Incident Reporting to Federal Government
- ✓ What Companies Should Be Doing to Prepare

Privacy+ Security Forum

SEC CYBERSECURITY INCIDENT RESPONSE RULES

Privacy+ Security Forum

The SEC adopted new disclosure requirements in July 2023 regarding cybersecurity risk management, strategy, governance and incident reporting for public companies.

- Incident Reporting
  - Real-time disclosure required of cybersecurity incidents on Form 8-K or Form 6-K, as applicable (FPIs).

- Disclosure Regarding Risk Management, Strategy and Governance
  - A description of their board of director's role in the oversight of risk stemming from cybersecurity threats, including the role of any committees or sub-committees therein.
  - A description of the management team's role and expertise in handling material cybersecurity risks.
  - Disclosures must be made on Form 10-K or 20-F as applicable (FPIs).

Incident Reporting requirements go into effect on December 18, 2023. Companies whose fiscal years end starting on December 15, 2023 will need to begin making the risk management, strategy, and governance requirements.

NYDFS PART 500 AMENDMENTS

Privacy+ Security Forum

The New York Department of Financial Services adopted an amendment to the Part 500 Regulations last week. Some highlights of the updated regulations

- Class A Companies: New obligations for companies with at least $20M revenue including independent audits by either internal or external auditors , vulnerability assessments, password controls, and monitoring.

- Governance: Boards role should play a prominent role in cybersecurity oversight including having a "sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors." CISOs are also required to report to boards on any material cybersecurity incidents

- Policies: New policies required around asset inventory, vulnerability management, and remote access, and updated policies for business continuity and incident response.

There will be a ramp-up period (18-24 months) for covered entities to demonstrate compliance.

CCPA SECURITY AUDITS AND ASSESSMENTS

Privacy+ Security Forum

The California Privacy and Protection Agency issued a rulemaking in September requiring certain businesses that fall under the CCPA to conduct both 1) annual cybersecurity audits and 2) cybersecurity risk assessments where processing personal data involves "significant risk to consumers privacy."

Annual Cybersecurity Audits	Cybersecurity Risk Assessments
✓ Format: Can be conducted internally or by a third party chosen by the business. ✓ Audit Topics: Most topics seen in cybersecurity audits including, but not limited to, access controls, authentication, assessment, hardware configuration, and incident response. ✓ Timing: Audits will need to be completed no later than 24 months after the rules are finalized.	✓ Scope: Draft rules define several areas where businesses would be required to conduct risk assessments, including, but not limited to: ○ Selling or sharing personal information. ○ Processing sensitive personal information. ○ Processing customer personal information for AI/automated decision-making purposes. ✓ Criteria: Draft rules provide several proposed elements of each risk assessment including describing in detail the processing activity and data used, along with benefits and negative impacts to the processing activity.

ARTIFICIAL INTELLIGENCE EXECUTIVE ORDER & RELATED DEVELOPMENTS

Privacy+ Security Forum

President Biden signed a sweeping Executive Order last week directing the Federal government to play a greater role in AI oversight, focusing on developing new standards/guidance and promoting new areas of research on AI use.

AI Standards (Sec. 4)	Privacy (Sec. 9)
• AI system developers must share safety tests of models that impact national security with Federal government. • Requires NIST to set new standards for testing AI systems ("red-teaming"). • Requires Commerce to develop guidance for "content authentication and watermarking," which will help classify AI-generated content. • Devote funding to the development of AI tools for fixing software vulnerabilities.	• Authorizes a new Research Coordination Network that will work with the National Science Foundation to research and invest in privacy technology. • Draft new guidance for Federal agencies to account for AI in collection and processing of personal data. • Encourage use of AI to enhance privacy-preserving techniques for processing personal data. • Call for a comprehensive privacy law (Fact Sheet).

DHS SECURE-BY-DESIGN GUIDANCE

Privacy+ Security Forum

CISA issued an updated version of its Secure by Design Guidance in October 2023. The original version released guidelines for manufacturers to build safe and secure software based on seven principles. Updates have resulted in revisions of the below principles:

- Take Ownership of Customer Security Outcomes
  - Establish default application settings for customers that allow for greater security protections.
  - Conduct more active field tests for software.

- Embrace Radical Transparency and Accountability
  - Publish more data and statistics regarding the safety of products, including software bills of materials, SLDC self-attestations, and high-level threat models.

- Lead From the Top
  - Provide disclosures in public reports on secure-by-design procedures.
  - Provide regular updates to board on security programs.

HARMONIZATION OF CYBER INCIDENT REPORTING TO FEDERAL GOVERNMENT

Privacy+ Security Forum

DHS released guidance last month proposing streamlining Federal government incident reporting requirements. Some recommendations included:

- Definitions: Federal agencies should agree to mutual terminology around incident reporting, including developing a common definition for “reportable incident.”

- Reporting: Federal agencies should agree on timelines for incident reporting, as well as streamlining the forms required, and timelines for submissions.

- Notices: Agencies should draft guidance on when notice to affected individuals of a security incident should be delayed for national security reasons.

WHAT COMPANIES SHOULD BE DOING TO PREPARE

Privacy+ Security Forum

- ✓ **Review incident reporting plans and ensure they comply with new regulations/laws.**
  - Roles and Responsibilities
  - Escalation Procedures
  - After-Action Reports

- ✓ **Review the people, processes, and tools that are driving cybersecurity operations and risk in your companies, and ensure they have the right expertise/acumen in place.**
  - Cybersecurity Board Governance
  - CISO Reports to Board
  - Third Party Audits

- ✓ **Review and update security settings for information systems.**
  - Encryption
  - Multi-factor Authentication