SentinelOne®

CHARLESTON
SCHOOL OF LAW

Charleston CyberLaw Forum

January 18, 2024

SentinelOne®

CHARLESTON
SCHOOL OF LAW

National Cyber Strategy: Implementation

Crowell

IST Institute for SECURITY + TECHNOLOGY

ActZero®

Presenters

Evan Wolff

Moderator
Crowell & Moring

Megan Stifel

Chief Strategy Officer
Institute for Security + Technology

Rob Knake

Head of Strategy
ActZero

SentinelOne®

CHARLESTON
SCHOOL OF LAW

Presentation Agenda

1. Overview of the National Cybersecurity Strategy
2. SEC Mandatory Cybersecurity Disclosure and Risk Management Rules
3. DFARS & 7012 History
4. New York Department of Financial Services Amendments

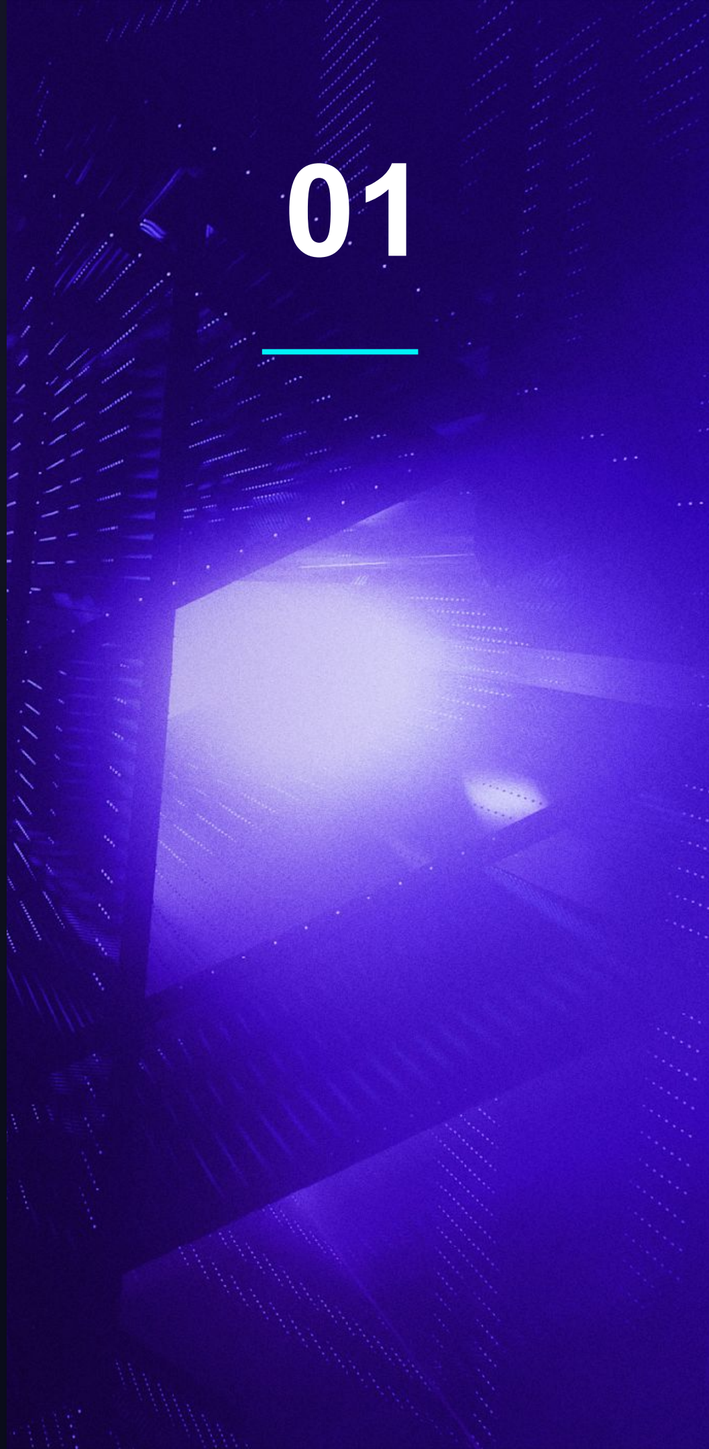
The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

SentinelOne®

CHARLESTON
SCHOOL OF LAW

01

Federal Cybersecurity Trends



The National Cybersecurity Strategy

The Biden Administration released the Strategy on March 2, 2023,
“to secure the full benefits of a safe and secure digital ecosystem for all Americans.”

Outlines 5 pillars:

1. **Defend Critical Infrastructure**
2. **Disrupt and Dismantle Threat Actors**
3. **Shape Market Forces to Drive Security and Resilience**
4. **Invest in a Resilient Future**
5. **Forge International Partnerships to Pursue Shared Goals**

SEC Mandatory Cybersecurity Disclosure and Risk Management Rules

Public companies (i.e., companies with securities registered with the SEC must now disclose in their Form 8-K Item 1.05 filings "material" cybersecurity incidents within four business days

- Information is material if "'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision, or if it would have 'significantly altered the 'total mix' of information made available'"

Companies must also describe their "processes" for identifying and managing cyber threats

- Do not have to disclose actual policies / procedures

New York Department of Financial Services

Revisions to 23 NYCRR Part 500 (the “Second Amendments”) released on November 1, 2023

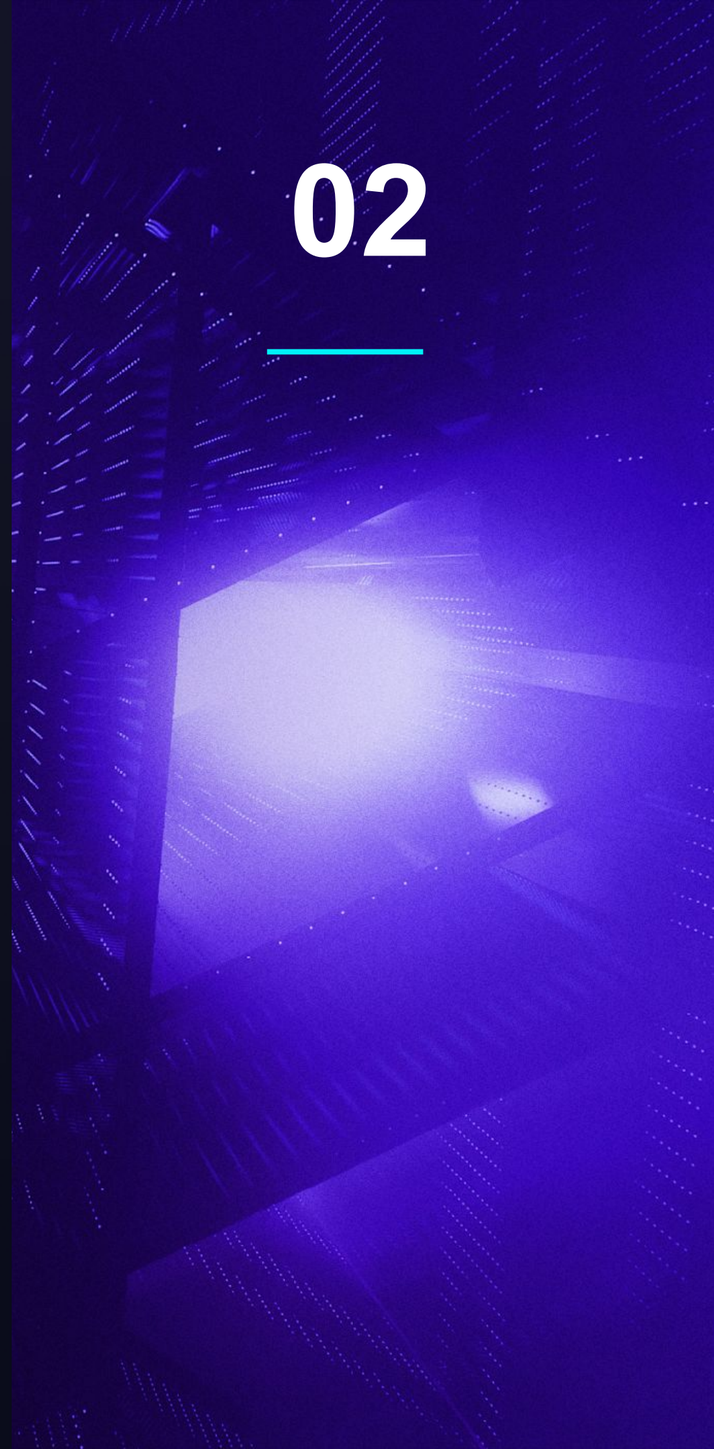
- Applies to “covered entities,” including “any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies”
- Requires covered entities “to assess its specific risk profile and design a program that addresses its risks in a robust fashion”

Program	**Policy**	**Governance**	**Vulnerability Management**
Audit Trail	**Access Privileges and Management**	**Application Security**	**Risk Assessment**
Personnel and Intelligence	**Third-Party Policy**	**MFA**	**Asset Management and Data Retention**
Monitoring and training	**Encryption of nonpublic information**	**Incident Response and Business Continuity**	**Notice**
Confidentiality	**Exemptions**	**Enforcement**	**Effective Date**

SentinelOne® CHARLESTON SCHOOL OF LAW

02

Federal Government Contracts Cybersecurity



Federal Cybersecurity Retrospective

2013 – 2016
Safeguarding CUI
DFARS 7012

Requires contractors to document compliance with NIST SP 800-171 or FedRAMP Moderate for cloud-based solutions

Contractors must report incidents affecting CUI

Must be flowed down to subcontractors

January 2020
CMMC
Introduced

Comprehensive CUI protection

Certification required before contract award

Compliance evaluated by third-party assessors

September 2020
NIST Basic Assessment
DFARS 7019, - 20

7019/20: requires self-assessment and scoring compliance with NIST SP 800-171

Enables government cyber audits

7021: CMMC certification requirement (inactive)

Must be flowed down to subcontractors

October 2021
DOJ Civil Cyber Fraud Initiative

DOJ announces that it will use False Claims Act (FCA) to enforce cyber noncompliance

Late 2024
CMMC Active
7021

DoD expects CMMC requirements finalized in late 2024

NIST SP 800-171 Draft Rev. 3 introduces new Supply Chain Risk Management control family

SentinelOne

CHARLESTON
SCHOOL OF LAW

Cyber Supply Chain Compliance Trends

National Cybersecurity Strategy Initiatives

Emerging Software Bill of Materials (SBOMs) Requirements

- FAR Proposed Rules on Incident Reporting (IR) and Federal Information Systems
- Secure Software Development Framework

NDAA Supply Chain Technology Requirements (e.g. FASCSA, circuit boards restrictions)

Increasing Supply Chain Requirements and Flow Downs

USG restricting products from certain companies of foreign origin (e.g., Russia, China)

- DHS Binding Operations Directives (BODs)
- National Defense Authorization Act (NDAA) Restrictions

Penalties for Noncompliance

- SEC Requirements
- Contract Termination
- Suspension and Debarment
- Poor Contract Performance Rating (CPARS)
- Removal / Replacement
- False Claims Act

SentinelOne

CHARLESTON SCHOOL OF LAW

CMMC 2.0 Proposed Rule

The Cybersecurity Maturity Model Certification Program (CMMC) proposed rule was released December 26, 2023 by the DoD, and includes 3 tiers:

- **CMMC Level 1:** Implement 15 controls listed in FAR Basic Safeguarding Clause 52.204- 21(b)(1) where Federal Contract Information (FCI) is handled
- **CMMC Level 2:** Implement 110 controls from NIST SP 800-171, Rev. 2 where Controlled Unclassified Information (CUI) is handled
- **CMMC Level 3**: Implement 24 select controls from NIST SP 800-172 plus full implementation of NIST SP 800-171 where high-value CUI is handled

Self-Assessments and Third-Party Assessments are determined by the government and align with the criticality of data:

- Self-Assessments require contractors to verify their own compliance with CMMC and submit their assessment score to the DoD's Supplier Performance Risk System (SPRS)
- Required annually for Level 1 and some Level 2
- Certification Assessments require an external third-party assessment
- Level 2 requires assessments by third-party assessment organization (C3PAO)
- Level 3 requires assessments by Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)
- Required every three years

CMMC 2.0 Proposed Rule

CMMC restricts POA&Ms depending on the Level

- No POA&Ms for Level 1
- POA&Ms allowed only for certain Level 2 and Level 3 security controls:
  - Point value is not greater than 1 (for Level 2)
  - Assessment score divided by the total number of security requirements is greater than or equal to 0.8, and
  - Control is not listed as ineligible POA&M control
- Contractors must close out POA&Ms (i.e., fully implement all pending controls) within 180 days of the initial assessment
- Failure to close out POA&Ms will result in contractual penalties and ineligibility for future contracts

Assessments may result in either Final Certification or Conditional Certification

- Final Certification obtained if contractor achieves minimum passing score
  and every required security control is fully implemented
- Conditional Certification obtained if approved POA&Ms exist upon completion of an assessment

Contractors must submit senior official affirmations attesting compliance for each CMMC Level

- Requires prime contractor and applicable subcontractor to annually affirm compliance with the controls
- Contractors must also affirm compliance after every CMMC assessment for CMMC Levels 2 and 3
  - Applies to both Self-Assessments, Certification Assessments, and after any POA&M close outs

DOJ Civil-Cyber Fraud Initiative

In October 2021 DOJ announced Civil Cyber-Fraud Initiative focused on civil enforcement against government contractors that fail to follow cybersecurity contract requirements.

DOJ "expect[s] whistleblowers to play a significant role in bringing to light knowing failures and misconduct in the cyber arena."

Initiative will utilize FCA to hold accountable contractors that knowingly:

- Fail to meet specific contract terms
- Misrepresent security controls and practices
- Fail to timely report suspected breaches

Exposure For Companies and Individuals:

- FCA liability can apply both to corporate entities and individuals
- Liability may arise if contractors fail to conduct a sufficient investigation of their cybersecurity practices and procedures prior to submitting self-assessment
- Liability may arise if contractors do not provide C3PAOs with accurate information about the scope of their covered contractor information systems – the boundaries where CUI resides

SentinelOne

CHARLESTON SCHOOL OF LAW

Evan Wolff

Partner, Crowell & Moring

Crowell

Evan D. Wolff is a partner in Crowell & Moring's Washington, D.C. office, where he is co-chair of the firm's Chambers USA-ranked Privacy & Cybersecurity Group and a member of the Government Contracts Group. Evan has a national reputation for his deep technical background and understanding of complex cybersecurity legal and policy issues. Calling upon his experiences as a scientist, program manager, and lawyer, Evan takes an innovative approach to developing blended legal, technical, and governance mechanisms to prepare companies with rapid and comprehensive responses to rapidly evolving cybersecurity risks and threats. Evan has conducted training and incident simulations, developed response plans, led privileged investigations, and advised on hundreds of data breaches where he works closely with forensic investigators. Evan also counsels businesses on both domestic and international privacy compliance matters, including the EU General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). He is also a Registered Practitioner under the Cybersecurity Maturity Model Certification (CMMC) framework.

Megan Stifel

Chief Strategy Officer, Institute for Security and Technology

IST Institute for SECURITY + TECHNOLOGY

Megan Stifel is the Chief Strategy Officer at the Institute for Security and Technology, where she also leads the organization’s cyber-related work. Megan previously served as Global Policy Officer at the Global Cyber Alliance and as the Cybersecurity Policy Director at Public Knowledge. She is a Visiting Fellow at the National Security Institute. Megan's prior government experience includes serving as a Director for International Cyber Policy at the National Security Council. Prior to the NSC, Ms. Stifel served in the U.S. Department of Justice as Director for Cyber Policy in the National Security Division and as counsel in the Criminal Division’s Computer Crime and Intellectual Property Section. Before law school, Ms. Stifel worked for the U.S. House of Representatives Permanent Select Committee on Intelligence. She received a Juris Doctorate from Indiana University and a Bachelor of Arts, magna cum laude, from the University of Notre Dame. She is a member of the Aspen Global Leadership Network as a Liberty Fellow.

Rob Knake

Head of Strategy, ActZero

ActZero

Rob Knake, served as Deputy National Cyber Director for Budget and Policy at the Office of the National Cyber Director (ONCD). Rob was a Fellow at Harvard's Belfer Center and a Senior Fellow for Cyber Policy at the Council on Foreign Relations. Rob served from 2011 to 2015 as Director for Cybersecurity Policy at the National Security Council. In this role, he was responsible for the development of Presidential policy on cybersecurity and built and managed Federal processes for cyber incident response and vulnerability management. Rob is co-author of Cyber War: The Next Threat to National Security and What to Do About It and the Fifth Domain: Defending Our Country, Our Companies and Ourselves in the Age of Cyber Threats.

Thank You

SentinelOne®

CHARLESTON
SCHOOL OF LAW

sentinelone.com