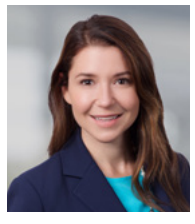
National Security: Evolving Risks for Corporations

Takeaways from S&C's podcast series featuring:

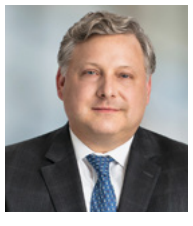
Andrew DeFilippis
defilippisa@sullcrom.com
+1 212 558 4000
>View bio



Nicole Friedlander
friedlandern@sullcrom.com
+1 212 558 4332
>View bio

Amanda Houle
houlea@sullcrom.com
+1 212 558 4000
>View bio

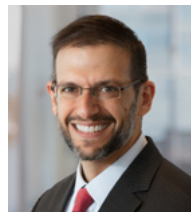
Craig Jones
jonescra@sullcrom.com
+44 20 7959 8900
>View bio



Eric Kadel
kadelej@sullcrom.com
+1 202 956 7500
>View bio

Sharon Cohen Levin
levinsc@sullcrom.com
+1 212 558 4000
>View bio

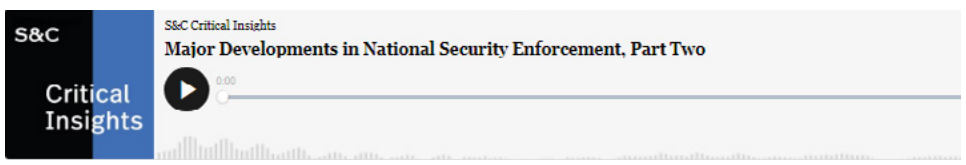
Tony Lewis
lewisan@sullcrom.com
+1 310 712 6615
>View bio



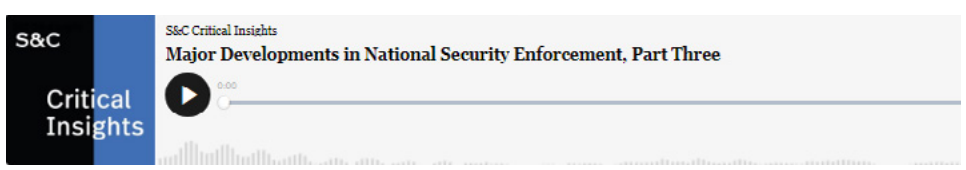
Adam Szubin
szubina@sullcrom.com
+1 202 956 7528
>View bio

Part 1: DOJ's increased focus on national security in the corporate context

Part 2 : Developments in voluntary self-disclosure and whistleblower programs



Part 3 : White House Executive Order on upcoming rules to protect data privacy in national security context



DOJ's Increased National Security Focus on Corporations

Companies operating in high-risk jurisdictions face an evolving risk, as the U.S. Department of Justice and other agencies have increased their focus on corporate activities in the context of National Security.

- DOJ's National Security Division recently named its first Chief Counsel for Corporate Enforcement, and is adding 25 attorneys to focus exclusively on national security-related economic crimes.
- The number of major DOJ corporate criminal resolutions implicating U.S. national security has more than doubled from 2022 to 2023 and the government has increasingly focused on strategic technology.
- DOJ has expanded its Bank Integrity Unit to target national security-related financial misconduct including money laundering, sanctions-related offenses and BSA matters.

Self-Disclosure and Whistleblowing

In July 2023, DOJ, Commerce and Treasury clarified those agencies' voluntary self-disclosure programs, including for sanctions and export controls.

- Be proactive: If you believe a transaction will likely come to the government's attention, it might be in your interest to disclose it.
- Consider the benefits of reporting: Companies now have increased incentives to report on others to avoid prosecution and penalties.
- Be alert to identifying the ultimate recipient of goods that you're exporting.
- Be aware that anonymity-enhancing tools in the crypto space have drawn enforcement activity recently (e.g., Tornado cash case).
- In the M&A context, be alert to identifying and promptly reporting misconduct at acquired companies in order to take advantage of a new safe harbor for acquiring companies.

Data Privacy

In February 2024, a White House Executive Order announced upcoming DOJ rules to protect data privacy in the national security context. These rules, yet to be issued, could create a sweeping new regime applicable to a broad range of companies and financial institutions.

- The pending regulations are not as comprehensive as the EU's GDPR. Rather, they address specific national security and privacy threats from five countries: China, Russia, Venezuela, Iran and North Korea.
- The DOJ will be the primary agency responsible for implementing the regulations.
- A wide range of companies will be required to monitor and restrict the flow of sensitive U.S. data to the effected countries.
- Due diligence protocols might be necessary to determine foreign ownership and ultimate beneficial owners of the companies to which you're transferring sensitive data.
- Penalties for violations will likely take into account the strength of a company's compliance program.

Learn more about **S&C's National Security Practice.**