A Growing Focus on Cybersecurity

Skadden

04 / 30 / 21

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Sahar Segal
Associate / Chicago
312.407.0539
sahar.segal@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

President Joe Biden has been fulfilling his promise to prioritize cybersecurity in his administration: He issued several cybersecurity-related executive orders, and federal regulators under his administration also have turned their focus to these issues. In its first 100 days, the administration has signaled an intent to collaborate with the private sector while also holding companies accountable through enforcement actions. Below are three trends we expect as the administration continues to pursue its cybersecurity agenda.

A Focus on Supply Chain Vulnerabilities

In the wake of recent high-profile attacks such as those involving SolarWinds, Microsoft's Exchange Server and Accellion, the federal government continues to increase its scrutiny of supply chain vulnerabilities and vendor oversight. President Biden signed an Executive Order on America's Supply Chains in late February 2021, requiring the departments of Commerce and Homeland Security to review supply chain risks in the information and communications technology sectors.

The administration has also indicated a desire to strengthen collaboration with the private sector. When forming a Unified Coordination Group for the Microsoft Exchange Server hack, for example, the administration included private sector members for the first time. It also announced plans to work closely with private internet and cloud service providers to gain greater insight into U.S. digital infrastructure, and Secretary of Homeland Security Alejandro Mayorkas emphasized the same in public remarks.

Despite working to strengthen public-private partnerships, federal regulators under the Biden administration are also expected to emphasize enforcement and focus on companies' diligence concerning supply chain risk. To avoid falling into the regulatory crosshairs, companies should consider reassessing their cybersecurity requirements for suppliers in light of recent attacks and incorporate those requirements into requests for proposal and contracts. Security teams should also continue to verify compliance with these requirements and work with vendors to promptly address any shortcomings.

Increased Cybersecurity-Related False Claims Act Enforcement

Government contractors face heightened risk of Department of Justice (DOJ) enforcement under the False Claims Act (FCA) due to an influx of new and updated government contract guidelines and requirements relating to cybersecurity and data privacy. Acting Assistant Attorney General Brian M. Boynton remarked in February 2021 that cybersecurity is a DOJ enforcement priority under the FCA, and practitioners have recently observed an uptick in cybersecurity-related FCA investigations. In the ongoing *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, for example, Aerojet is alleged to have falsely certified compliance with Department of Defense and NASA cybersecurity standards in order to obtain contracts. Given a heightened risk of FCA enforcement, government contractors and their subcontractors should ensure compliance with evolving federal cybersecurity requirements and remedy any shortcomings.

Heightened Threat of Ransomware Sanctions

Ransomware attacks continue to grow in frequency and sophistication. Many companies do not realize, however, that making a ransom payment in order to restore their systems may subject them to Office of Foreign Assets Control (OFAC) enforcement under the guidance it issued in October 2020. A more active OFAC department under the Biden administration is likely to identify opportunities to follow through on its warnings. Companies can minimize the risk of OFAC civil monetary penalties by implementing and regularly updating a cybersecurity-focused, risk-based sanctions compliance program and by exercising diligence before making any payments to ransomware threat actors.