Blogs
February 08, 2023
Perkins on Privacy

Biden Administration Plans Mandatory Cybersecurity Regulations for Critical Infrastructure Companies

Recent comments by Anne Neuberger, President Biden's Deputy National Security Adviser for Cyber and Emerging Technology, herald an important shift in U.S. cybersecurity policy. Traditionally, the U.S. Government's approach has mostly focused on requiring companies to notify regulators and affected individuals of security breaches that implicate specific types of information, such as personally identifiable information, protected health information, and financial information. Federal efforts to prescribe or enforce proactive security measures have been sector-specific, such as the Transportation Security Administration's Security Directives covering rail and pipeline owners and operators. Those measures have been spread among sector-specific agencies, which has resulted in multiple, and sometimes conflicting or confusing, requirements applying to some businesses. Federal law enforcement agencies have also made targeted and novel use of criminal search authorities to proactively remediate privately owned machines infected with malware by Russian and China-based actors.

According to press reports, that may be about to change. The new National Cybersecurity Strategy will likely change the U.S. Government's structural and substantive approach. The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security will play an increasingly central role while drawing on the subject-matter expertise of sector-specific agencies. And the government will start issuing cybersecurity mandates to the private sector, rather than merely encouraging security and requiring reporting. Agencies reportedly will rely on existing authorities when they can and seek additional powers as necessary. Ms. Neuberger's statement that *voluntary* efforts "have been insufficient against the threat to the critical services Americans rely on" seems to confirm these reports. Accordingly, private-sector entities, particularly those in critical infrastructure and related supply chains, should expect to see mandatory cybersecurity requirements rolling out in 2023.

Regulation of cybersecurity in the private sector raises concerns of added costs, requirements that lag behind developments in threats and technology, and duplicative, irrelevant, or counterproductive mandates. But while a national strategy document is an important beginning and a significant announcement of a new direction for Executive Branch agencies, there may be a longer road ahead for implementation of specific measures. If DHS's approach in issuing regulations under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), and even recent revisions to TSA's requirements for rail security, are any indication, federal regulators will look for cooperation from the private sector. It would not be surprising if federal cybersecurity officials seek input from industry regarding best practices and on approaches that will enhance security without unduly interfering with company operations – in contrast to a checkbox-based, compliance-centric approach that layers regulatory obligations on top of a company's own cybersecurity efforts. If that is the case, industry should take the opportunity to engage fully with security officials to maximize the likelihood that federal efforts will promote, and not impede, security in critical infrastructure and throughout the economy. Companies should work with counsel to identify opportunities to help shape forthcoming regulatory regimes. Counsel can also help companies prepare to meet new requirements by reviewing current data security programs, conducting gap analyses, and ensuring that governance documentation is complete and up to date.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog