President Biden Calls on Private Sector Businesses to Implement Heightened Cybersecurity Risk Protocols

Client Alert

3.25.22

What You Need to Know

- President Biden has called upon private sector businesses to take specific steps to implement certain “best practices” aimed at minimizing their cybersecurity risks in light of heightened concerns about possible Russian cyberattacks on U.S. targets.
- A related Fact Sheet published by the White House notes that much of the nation’s critical infrastructure is owned and operated by the private sector, which has “the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely.”
- Private sector businesses of all sizes should proactively seek to upgrade system safeguards and develop protective business policies and procedures to address cybersecurity-related challenges in this time of heightened risk.

By: Meredith C. Sherman

On March 21, 2022, the White House issued a "Statement by President Biden on our Nation's Cybersecurity" which calls upon the private sector to "harden [their] cyber defenses immediately." The President's remarks send a clear message to private companies that defense against Russian or other cyberattacks will require collaboration and cooperation between members of both the public and private sectors.

It is critical that businesses of all sizes, operating across a comprehensive range of industries, proactively take quick action to minimize potential exposure to evolving cybersecurity and compliance risks. To ensure compliance with a rapidly changing landscape of cybersecurity-related laws and regulations, business owners and

other decision-makers should seek out the guidance of internal or external legal counsel, information technology specialists, and cybersecurity professionals when taking steps to address the issues outlined in President Biden's statement and accompanying Fact Sheet, as summarized below:

- Private sector entities are encouraged to take specific steps to implement acknowledged "best practices." These include the use of multi-factor authentication, the deployment of modern security tools, collaborating with cybersecurity professionals to protect systems against vulnerabilities, backing up data including the use of offline backups, running emergency plans and incident response exercises in preparation for and in advance of a potential attack, encrypting data, continuing to train and educate employees, and engaging proactively with local FBI or Cybersecurity & Infrastructure Security Agency (CISA) Regional Officers to establish relationships in advance of any potential incidents.
- Technology and software companies are further encouraged to continuously scan for known and potential vulnerabilities and to implement the security practices of the President's May 2021 Executive Order 14028, Improving our Nation's Cybersecurity.
- The Fact Sheet notes that much of the nation's critical infrastructure is owned and operated by the private sector, which has "the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely." The Fact Sheet comments additionally that the federal government will continue its efforts to provide resources and tools to the private sector, including via the CISA Shields Up Campaign.

The statements issued by the White House dovetail with the Strengthening American Cybersecurity Act of 2022, bi-partisan legislation that was signed into law by President Biden on March 15, 2022. The Act includes provisions that seek to protect critical infrastructure in the U.S. by requiring certain types of companies to report cybersecurity incidents to a federal agency within 72 hours of discovery, and to report any ransomware payment within 24 hours.

Given the heightened potential for malicious cyberactivity in response to economic sanctions imposed on Russia by the U.S. following the military invasion of Ukraine - and in light of the plethora of both existing and proposed regulations - it is imperative for private sector businesses to assess and understand their cybersecurity risk profile. Businesses must take the necessary steps to upgrade system safeguards, focus on intensive workforce training and education, and develop and implement protective business policies and procedures to address cybersecurity-related challenges in this time of heightened risk.

Please contact the author of this Alert, Meredith C. Sherman, with any questions or to discuss your specific business circumstances.

Related Attorneys

Meredith C. Sherman

Partner

732.476.2672

Email