Published on *The National Law Review* https://natlawreview.com

Key Takeaways from President Biden’s Cybersecurity Executive Order

Article By:

Colin R. Jennings

Ericka A. Johnson

Ludmilla L. Kasulke

Over the last week, Americans have been riveted by scenes of panic buying at the pump after a ransomware attack shut down the Colonial Pipeline, a critical source of fuel for the entire East Coast. For the first time, many are reflecting on the national security implications of cybersecurity attacks on everyday life – and the US government is responding. On May 12, 2021, President Joe Biden signed an Executive Order (EO) on “Improving the Nation’s Cybersecurity,” signaling potentially increased regulatory oversight of cybersecurity laws and regulations.

The EO responds to recent high-profile cybersecurity attacks, including the most recent Colonial Pipeline incident. On May 7, Colonial Pipeline announced that a cyberattack forced the company to proactively close down operations and freeze IT systems. The Georgia-based company provides roughly 45% of the East Coast’s fuel, transporting more than 100 million gallons of fuel daily from Texas to New York – and the shutdown soon resulted in shortages and panic buying across the Southeast in particular.

During a May 13 press conference, President Biden assured the American public that fuel lines would soon be restored. However, the President noted that “it is clear to everyone that we need to do more than what we are doing now and the federal government can be a significant value added in making that happen.”

The President announced that the new EO “calls for federal agencies to work more closely with the private sector – to share information, strengthen cybersecurity practices, and deploy technologies that increase resiliency against cyberattacks.” Accordingly, the EO aims to make significant contributions to modernizing the federal government’s cybersecurity practices, particularly its software security, and under an aggressive timeline.

Broadly, the EO:

- Creates new IT security rules for select federal contractors – The EO directs revisions to the

Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplementation (DFARS) applicable to federal contractors that provide information technology, operational technology, and information and communications technology to the federal government. These revisions generally will remove contractual barriers to sharing information about threats, incidents and risks, etc., and require, among other things, prompt reporting of cyber incidents within 72 hours.

- Requires federal agencies to implement additional IT security measures – Those measures include, among other things, requiring agencies to accelerate movement to secure cloud services, evaluate the types and sensitivity of their unclassified data and develop secure storage solutions, adopt multifactor authentication and encryption to the maximum extent practical, and establish training programs.

- Sets standards for commercial software – The EO directs the establishment of baseline security requirements based on industry best practices and aims to develop a labeling methodology that manufacturers can use to inform consumers about the security of their software products. Further, the EO aims to leverage federal buying power to jumpstart the market for secure software by requiring that all software purchased by the federal government meets these standards.

- Creates a national review board – The EO establishes a Cyber Incident Review Board that will convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity going forward. Consistent with the Biden administration's focus on bringing in and partnering with the private sector on cybersecurity, the Cyber Incident Review Board will have a private sector co-chair

- Standardizes the government's incident response plan – The EO directs the development of a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activities.

While announcing the EO, the President argued that the US is competing with the world economically, adding, "we're not going to win it competing with an infrastructure that is out of the 20th century. We need a modern infrastructure." Likewise, the former US Secretary of Transportation, Rodney E. Slater, noted that "this administration is taking the timely lead to make significant investments in our digital infrastructure and make the bold changes necessary to secure America's national security interest."

Biden officials will continue prioritizing cybersecurity and its respective enforcement of cybersecurity laws and regulations, as means to continue to protect the everyday American and the country's economic recovery more broadly. For companies of all sizes, industries and locations, this means ensuring that your organization has conducted due diligence to mitigate the risk of, and be prepared to respond to, cyberattacks as they arise.

National Law Review, Volume XI, Number 138

Source URL:https://natlawreview.com/article/key-takeaways-president-biden-s-cybersecurity-

executive-order