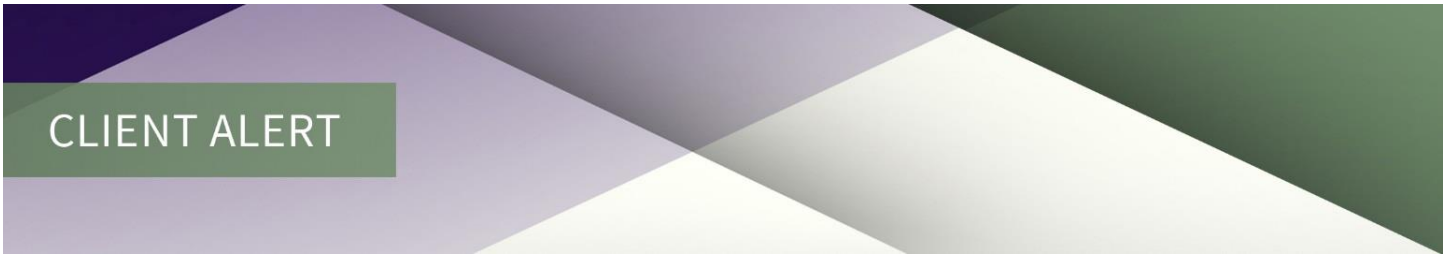

Cybersecurity Executive Order Uses Multiple Levers to Improve Cyber Posture

May 18, 2021

AUTHORS

Daniel K. Alvarez | Richard M. Borden | Elizabeth Bower | Elizabeth P. Gray | Laura E. Jehl

On May 12, 2021, President Biden signed a long-awaited Executive Order on Improving the Nation's Cybersecurity (the "Executive Order" or the "Order").[1] The Order is intended to address the threat to U.S. public- and private-sector entities presented by "persistent and increasingly sophisticated malicious cyber campaigns."[2] Rather than directing federal government agencies to impose any regulatory solutions or proposing any legislative fixes, the Executive Order seeks to leverage alternative sources of authority to encourage improved cybersecurity hygiene and behavior. In particular, the Order lays out significant changes to the way the federal government will purchase and use information and communications technology ("ICT") products and services, including changes that will impact the supply chain for those products and services. In addition, the Order leverages the federal government's convening power, directing National Institute of Standards and Technology ("NIST") to work with various agencies and the private sector to establish guidance on a number of key issues.

While the immediate impact is likely to be felt most directly by ICT companies that do business with the federal government, the Order potentially has implications even for companies that do not do business with the federal government. For example, the Order directs the creation of guidance on software supply chain security and the creation of a consumer-labeling pilot program regarding the security of Internet of Things ("IoT") devices and consumer software. These efforts could lead to standards that become industry norms or baseline expectations for ICT companies regardless of whether they contract with government entities, or could even be adopted or integrated into the cybersecurity

[1] Executive Order on Improving the Nation's Cybersecurity, May 12, 2021, available here.

[2] *Id.* § 1.

policymaking and enforcement efforts of agencies like the Securities and Exchange Commission, the Federal Trade Commission, and the Commodities Futures Trading Commission. In this Client Alert, we identify some of the key directives in the Order, as well as several issues and questions the Order raises.

BACKGROUND

Starting with the revelation in December 2019 that SolarWinds' Orion software platform had been compromised and culminating most recently with the ransomware-induced shutdown of the Colonial Pipeline, the last six months have seen a steady stream of major cybersecurity incidents. Until the Colonial Pipeline incident, a common characteristic of each attack was that the perpetrators gained access to major private-sector and public-sector systems by compromising a private-sector software platform — e.g., SolarWinds Orion, Microsoft Exchange, and Pulse Secure's VPN product. The Order directly responds to the strategies and tactics underlying these attacks, and in the process seeks to improve the nation's cybersecurity posture overall by focusing on how government agencies and actors can help reduce cybersecurity risk through best practices – not by imposing general regulatory requirements or calling for any new legislation.

IMPROVING CYBERSECURITY THROUGH THE GOVERNMENT'S PURCHASING POWER

In light of the fact that many significant recent cyber attacks have targeted government systems by infiltrating private-sector software and services, the Executive Order is focused primarily on the government's use of private-sector produced ICT products and services, particularly cloud services. In particular, the Order directs:

- Relevant government agencies to establish a number of contractual obligations and requirements in the Federal Acquisition Regulation ("FAR") regarding record keeping, reporting, transparency, and supply chain security. For example, the Order directs the agencies to recommend changes to ensure that private-sector service providers share data, information, and reporting related to cyber incidents or potential incidents relevant to any agency with which they have contracted, and that the service providers collaborate with federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents involving federal systems.[3]

- Federal agencies to amend their cybersecurity strategies to adopt certain practices, including: accelerating movement to secure cloud services; centralizing and streamlining access to cybersecurity data; and investing in both technology and personnel to match these modernization goals.[4]

[3] See, e.g., *id.* §§ 2(c), 2(i).

[4] *Id.* § 3(a).

- That "the migration to cloud technology shall adopt Zero Trust Architecture, as practicable," and that relevant agencies must work with the Federal Risk and Authorization Management Program ("FedRAMP") to develop security principles governing cloud providers for incorporation into agency modernization efforts.[5]

- That agencies must adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws.[6]

One of the major challenges presented by these directives is timing. While changes to the FAR can sometimes take years, the Order directs many of these changes to be proposed or released within 60, 90, or 180 days. The agencies tasked with leading this effort — like the Cybersecurity and Infrastructure Security Agency ("CISA") — are already busy on numerous other priorities and may need additional resources to get these directives over the finish line. Moreover, these changes include the need to define key concepts, such as "cyber incident," and other terms that could have broader implications for policymaking outside the context of government contracts. To do so, policymakers will need to juggle input and lobbying from a variety of stakeholders, but the process for doing so is unclear. Additionally, adopting advanced cybersecurity technologies may prove challenging to implement at the scale of federal agencies, especially in environments with large legacy infrastructure and ICT footprints.

IMPROVING CYBERSECURITY THROUGH CONVENING POWER

The Executive Order also seeks to encourage improved cyber hygiene and posture by leveraging the government's convening power. The Order directs the National Institute of Standards and Technology ("NIST"), CISA and other agencies to establish guidance and standards, and in so doing, seeks to bring interested stakeholders together to ensure that the standards account for their interests. Among other things:

- *Software Supply Chain Security.* The Order directs NIST to adopt guidelines for "enhancing software supply chain security."[7] The guidance should address secure software development environments and mechanisms for demonstrating the security of such environments, including by employing automated tools to perform functions like maintaining trusted source code supply chains and checking for known or potential vulnerabilities (and remediating, as appropriate), and providing a purchaser a "Software Bill of Materials" for each product directly or by publishing it on a public website.[8]

---

5 *Id.* § 3(c).

6 *Id.* § 3(d).

7 *Id.* § 4(c).

8 *Id.* § 4(i).

- *Consumer Labeling Pilot Program.* NIST is directed to coordinate with the FTC and other agencies to develop consumer-labeling pilot programs for IoT devices and consumer software. Per the Order, the criteria for the labeling program should "reflect increasingly comprehensive levels of testing and assessment that a product may have undergone."[9] Notably, the Order seems to recognize that industry participation may be an issue: "This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."[10]

- *Cyber Review Board.* Finally, the Order creates a new Cyber Safety Review Board charged with reviewing and assessing significant cyber incidents. The Board would be comprised of both federal government and private-sector representatives. Reports indicate that the Biden Administration views the creation of the Board as an effort to replicate in the cyber world the success that the National Transportation Safety Board has had in investigating major incidents involving automobiles, airplanes, and other forms of transportation.

As with the proposed changes to contract language and the FAR discussed above, the Order imposes aggressive timelines for NIST and other agencies to act, even while it delegates some thorny definitional and scoping questions. However, unlike the changes to contract language and the FAR, the Order has no clear jurisdictional hook to compel or incent participation in these efforts. While the Order will likely ensure that private sector interests are represented as these guidelines, programs, and even the Board are developed (especially considering that these may lead to standards that become industry norms or expectations), it remains unclear how or whether these efforts will have widespread impact barring some legislative or regulatory action.

CONCLUSION

After months of waiting to learn what the Biden Administration might do with respect to cybersecurity, the resulting Executive Order raises as many questions as it answers. For ICT companies that do business with the federal government, there will be a clear imperative to participate in the process as NIST and the other agencies hone in on the finer points of implementing the directives in the Order and craft guidelines and standards. In the absence of concerted legislative or regulatory action, however, it is unclear whether these efforts will gain traction or have any long-term effect on the broader cybersecurity environment.

[9] *Id.* §§ 4(s)-(v).

[10] *Id.* § 4(s).

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	Richard M. Borden	Elizabeth Bower	Elizabeth P. Gray	Laura E. Jehl
202 303 1125	212 728 3872	202 303 1252	202 303 1207	202 303 1056
dalvarez@willkie.com	rborden@willkie.com	ebower@willkie.com	egray@willkie.com	ljehl@willkie.com