Biden Cybersecurity Order's Biggest Impact: Software Supply Chain
Bloomberg Law
Alex Iftimie and Miriam Wugmeister
May 28, 2021
[Link]

President Joseph Biden's recent executive order on cybersecurity will leave its biggest mark on software supply-chain security, says Morrison & Foerster attorneys Alex Iftimie and Miriam Wugmeister. The order directs the National Institute of Standards and Technology to establish guidelines for secure software development for government suppliers that are likely to become private sector industry standards, they say.

The driving force behind the Biden administration's executive order on improving the nation's cybersecurity was the recent SolarWinds breach. The breach allowed the Russian intelligence service to get into the systems of at least nine federal agencies and numerous prominent private-sector companies via a software supply-chain hack that exploited SolarWinds software updates.

This unprecedented breach – as well as subsequent compromises of vulnerabilities in Microsoft, Accellion, Pulse Secure, and other software products – led to a renewed and urgent focus by government officials and the private sector on how to mitigate software supply-chain risk and protect their networks when the initial attack vector is a trusted piece of software.

The executive order's software supply-chain provisions reflect the government's largest step yet in addressing software supply-chain risk and could have widespread impact on the private sector.

Notification and Information Sharing Provisions Focused on Federal Contractors

Although there are a number of ambitious reforms in the executive order, many of its requirements apply only to the federal government.

Other requirements – like the mandatory notification and information-sharing provisions – only apply to the extent that a company contracts with the federal government. Even then, the federal contractor requirements will be implemented over time because they require modifications to government contracting regulations that will take time to draft and subsequently roll out into new contracts with the private sector.

The executive order's software supply-chain provisions are a different story. Those provisions direct the creation of new standards for enhancing software supply-chain security and leverage the buying power of the federal government to incentivize compliance across the software market.

Far-Reaching Software Supply-Chain Provisions

The executive order directs the National Institute of Standards and Technology (NIST) to develop guidelines for secure software development with which all commercial suppliers to the government will have to comply, and which are likely to become a standard that others adopt voluntarily.

These standards will have far-reaching impact because the federal government buys many of the same software products that the rest of us use. The government's software vendors include hundreds of companies, including well-known names such as Cisco, IBM, Microsoft, SAP, and Workday. And, because software developers are likely to use one software development process across their organization and products, all private-sector customers will benefit from those enhancements.

The supply-chain security rules will include baseline standards for software development environments such as the use of administratively separate build environments, multi-factor authentication, and data encryption.

The rules will also require vendors to maintain a vulnerability disclosure program and make public the results of automated security checks. And the rules will give new life to efforts to require vendors to prepare a software bill of materials, which is akin to an ingredient list for software components.

NIST Standards Likely to Become Industry Standards

Whether a company sells software to the government or not, the new NIST standards are likely to become the industry standard and will be emulated across the private sector. We've seen this play out before.

In 2013, President Obama issued an executive order on improving critical infrastructure cybersecurity, which called on NIST to develop a voluntary risk-based cybersecurity framework for the nation's critical infrastructure.

That framework – which sets out industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks – has become a common framework used by private-sector entities across industries to benchmark cybersecurity programs and chart planned improvements.

We expect that the software supply-chain standards that emerge from NIST are likely to become a common standard by which software supply-chain security is measured, and incorporated into minimum requirements that customers are likely to demand. So, if there's an area of the executive order for the private sector to focus on, the requirements around secure software development are surely it.

More Private-Sector Impacts

There are, of course, other ways in which Biden's executive order will impact the private sector indirectly. As the government throws its weight toward using secure cloud infrastructure, cloud providers will be incentivized to provide services that are more secure and that give the government (and ultimately private-sector customers) more control.

Similarly, as more private-sector companies share information with the U.S. government regarding cybersecurity incidents, there will be continuing pressure on the U.S. government to share insights and threat intelligence that it accumulates back with the private sector, including those who do not directly contract with the U.S. government.

Also, although the executive order's breach notification requirements will be limited to federal contractors, there are already calls from members of Congress and others for a national breach notification law that would apply across the private sector.

Recent incidents like the SolarWinds compromise have put a spotlight on the risk posed by state-sponsored and criminal efforts to target global companies through supply-chain hacks. It's a national security and business risk that merits attention. The standards and rules that emerge as a result of the executive order will help provide a common framework for mitigating that risk and a financial incentive for companies that elect to participate.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Alex Iftimie is a partner and co-chair of Morrison & Foerster's Global Risk + Crisis Management practice group. He is a former Department of Justice national security official. He is based in San Francisco.

Miriam Wugmeister is partner and co-chair of Morrison & Foerster's preeminent Privacy + Data Security practice group. Some of the world's largest and most complex organizations regularly call on her to confront their most difficult U.S. and international privacy challenges. She is based in New York.