Beyond Compliance

Biden's Executive Order on Improving the Nation's Cybersecurity, Explained

On May 2021, President Joe Biden announced the **Executive Order on Improving the Nation's Cybersecurity**, paving a path forward to help agencies and policymakers modernize the nation's federal agencies against evolving cyber attack. This directive comes after a rapid and intense spike in significant cyber incidents, from the SolarWinds breach to the Colonial Pipeline hack. With a 30-60-90 day timeline, there's a sense of urgency throughout the executive order — and for good reason. Agencies must move quickly to prevent the next cyberattack.

That's not an easy task, especially as cyber threats become increasingly sophisticated, as do computing environments.

"There are new technologies out there," says Meghan Good, Director of the Cyber Accelerator at Leidos. "There are different environments. We've really moved beyond the perimeter and we now have technologies running our business and operations that no longer reside in a physical location. There's increasing risk and a need to secure that further."

A new executive order aims to improve the nation's cybersecurity. Here are some steps agencies can take now to put these cybersecurity initiatives front and center.

The Brave New World of Cybersecurity

The challenges seem daunting; organizations can feel like a minor flaw can expose droves of sensitive information. And with the move to cloud services, the organizations are having to trust their providers to securely manage their infrastructure, instead of keeping it within their own walls.

Even though the control shifts, in some ways, the move to cloud also brings better tools that enable much more granular control and visibility at scale. Cloud capabilities combine with identity credential and access management, or ICAM, tools to keep out malicious actors. A modernized cloud approach also looks past broad network perimeters we think of today and is replaced by a set of micro-perimeters inside the network that are inclusive of identity.

"It's not just human users that we need to be concerned about," says Lakshmi Ashok, who leads the development of multi-cloud enterprise management and governance capabilities at Leidos. "The growing need to [verify] digital identities also extends to machine-like devices. You have things like the Internet of Things and workloads like containers and serverless technologies that you need to secure. These are some of the paradigm shifts that we need to be concerned about."

Adopting a zero trust architecture based on the belief that organizations shouldn't automatically trust anything or anyone attempting to access their systems will be key to staying secure.

“There are new technologies out there. There are different environments. We’ve really moved beyond the perimeter and we now have technologies running our business and operations that no longer reside in a physical location. There’s increasing risk and a need to secure that further.”

Meghan Good

Director of the Cyber Accelerator, Leidos

Few industry experts understand this better than Jeff Mims. As a chief technologist at Leidos, he educates public sector customers and stakeholders about zero trust adoption. The executive order is a step in the right direction to raise awareness about zero trust, he says.

“From my perspective, I was spending a lot of time explaining what zero trust is,” Mims says. “So I did appreciate that the executive order gave a very good explanation of zero trust architecture and how it applies.”

However, agencies eager to start implementing zero trust initiatives may not necessarily have the funding to do so, he noted.

“One thing that I’ve heard the most is this didn’t come with funding, but it came with a whole lot more work,” Mims says. “So we have to find creative ways to fund these cybersecurity initiatives.”

A Call for Collaboration

Information sharing between government and industry will become more routine as agencies adopt new guidelines and best practices. In fact, the executive order pushes service providers to share additional threat data and report cyber incidents to more than just the agencies they work with but also to other agencies involved in cyber response.

This could lead to a shift away from the siloed approach to incident response that has complicated the government’s efforts to intervene to investigate and help companies.

Many industry experts were surprised to see the level of greater information sharing make its way into the executive order.

“I would never have thought the government would call upon cloud solutions providers to actually share information on cyber incidents in a real-time or near real-time basis,” Ashok says.

It could be a step in the right direction, but it will require active engagement between government and industry in implementing the executive order. The government will need to partner with the private sector to develop strong mechanisms to quickly and efficiently categorize and review the additional cyber threat and incident information received to ascertain which threats are imminent and significant. They must also critically determine how to get threat information packaged back to industry in a timely fashion, without overburdening the private sector with ambiguous or costly new requirements or negatively impacting the confidentiality of proprietary and other protected information. This will require additional effort by the government to understand the practical effect of its rules and listening to a broad range of perspectives including the input of large contractors, small businesses, commercial companies and non-traditional government contractors. But with so many government contractors entering the cybersecurity space, greater collaboration with industry can seem overwhelming for an agency in both rulemaking and technology.

"It's a very crowded landscape in terms of cybersecurity capabilities and technologies out there," Mims says. "And it makes it somewhat confusing and inundating, especially when you have a lot of vendors coming to you. Working through product and service vendors is challenging even for us and other system integrators. It's even more so for government officials who are trying to promote fair competition and trying to understand where their capabilities fit. And the government is also trying to adopt an approach that doesn't require them to rip out large chunks of hardware and software and make major changes that could introduce risk to the current mission."

His advice to agencies? Understand the mission and develop a roadmap for your specific needs and requirements. Those requirements will likely change alongside the evolving threat landscape, so organizations must remain resilient and be ready to pivot as new threats arise.

A Move Toward Experimentation

It's not always easy to understand which cybersecurity products or services are necessary to solve a specific challenge. Mims advises agencies to leave room for experimentation as they attempt to connect the dots between a problem and a solution.

For starters, prioritize pilot efforts. A greenfield environment offers the opportunity to experiment and understand where specific products fit in.

"Even as experts in the [cybersecurity] community, we often have difficulty understanding exactly where a vendor's offering fits in," Mims says. "We start to see value, but we don't quite know how it's going to interact with other products and other services until we test it. So testing and iterating is really important before major decisions are made."

Amid an increasingly complex threat landscape, experimentation can be especially useful in attempting to understand the intent of the adversary. Leidos' software factories, for example, evaluate their own solutions from the perspective of a threat actor by incorporating security into the development and operations process.

"We're constantly thinking about how we move beyond compliance and the security controls within the software that we produce," Good explains. "We really try to take a look at our solutions and our software and see from an adversary perspective, from a threat-informed perspective, how the solutions might be vulnerable and address the vulnerabilities early and often through our SecDevOps processes and tools."

Indeed, no single solution can perfect your cybersecurity posture. Instead of seeing security as a box to check, Good recommends treating it as an ongoing, iterative process.

"It's all about figuring out what that roadmap is and realizing you're on a journey," she says. "You might not quite know where you're starting, but start, and then move forward from there."