Contact:
Rashi Ratan
rratan@meritalk.com
703-883-9000 x139

One Year In, Cyber Executive Order Progress is Under Way, But Early Stage

Significant percentage of decision-makers expect to see impact within the next year

Alexandria, Va., May 5, 2022 – Ninety-one percent of Federal cybersecurity decision-makers say the 2021 Executive Order (EO) on Improving the Nation's Cybersecurity has made U.S. data and critical infrastructure safer, but just 28 percent say significantly safer, according to *Impact Assessment: Cyber EO Year One*, a new study from MeriTalk, a public-private partnership focused on improving the outcomes of government information technology (IT).

The report explores perspectives on progress against Cyber EO goals, identifies what successful agencies do differently, and finds the fault lines where agency cyber leaders say they need more help to succeed. Most Federal cyber decision-makers (78 percent) agree the steps outlined in the Cyber EO are necessary to protect our nation. Implementing software supply chain security and migrating to a zero-trust architecture are the two most important factors for national cybersecurity, the research highlights.

And, while just 15 percent have seen tangible improvements because of EO efforts to date, a significant portion expects to see an impact within the next year.

Federal cyber leaders confirm initial progress in areas including vulnerability detection, software supply chain security, vulnerability response, and investigative and remediation capabilities. Just over half confirm IT management and staff are placing increased priority on cybersecurity, and just over half are collecting more cyber data than in the past. But, across the board, progress against EO goals is still in the early stages. Fewer than half rate their agencies' progress against key EO goals as "excellent." For example, 36 percent rate progress toward creating a formal strategy as excellent; 34 percent rate progress toward investing in endpoint detection and response (EDR) as excellent; and, 33 percent rate progress migrating to secure cloud solutions, as excellent.

When asked about the importance of zero trust, 82 percent agree that allocating staff and budget resources to zero trust is vital to national security and almost all, 96 percent, agree the Federal zero trust strategy is somewhat or very helpful. Despite the high priority, just 30 percent of Federal cyber decision-makers rate their zero trust progress as "excellent" and many, 67 percent, say the EO's three-year window for implementing a zero trust architecture is not realistic.

"Zero Trust is the gold standard for cybersecurity, so we're encouraged to see the EO is prioritizing that approach," said Drew Bagley, vice president and counsel for Privacy and Cyber Policy, CrowdStrike. "In addition, cloud-native endpoint detection and response capabilities can significantly strengthen the cybersecurity posture for the federal government, especially when integrated with other security capabilities including identity security, threat intelligence, and managed threat hunting. These concepts have become

-more-

cybersecurity best practices for the private sector's most technologically advanced businesses, and we encourage the public sector to continue to embrace these technologies and strategies."

"Getting to zero trust is not easy. The detail provided in the multi-step guidance from OMB provides a path, but there is no single box you can buy to meet the varied needs of the five zero trust pillars," says Stephen Kovac, Chief Compliance Officer and Head of Global Government Affairs, Zscaler. "You need multiple solutions from varying vendors that work together with seamless integration to achieve true zero trust – it is a team sport. OMB has done a good job in helping to define those rules, with rule one being to keep users off the network. If they can't reach you, they can't breach you."

Funding is another roadblock. Just 14 percent report they have all funding needed to meet Cyber EO requirements. One-third say they have half, or less than half, of the funding needed.

"The sea change is the focus on comprehensive cyber resiliency," says Nicole Burdette, principal, MeriTalk. "The EO provided direction, and Federal cyber leaders are now doing the hard work. But progress requires sustained funding and resource commitment. The research shows the gaps."

"The U.S. federal government is taking important steps to improve the nation's cybersecurity posture," said Dave Levy, Vice President of U.S. Government, Nonprofit, and Healthcare at Amazon Web Services (AWS). "In the Cyber EO, the White House directs federal agencies to adopt security best practices, implement zero trust architectures, and accelerate migration to secure cloud services. Organizations of all sizes should consider similar principles and practices to enhance their cybersecurity and protect employees and sensitive data against cyberattack."

What are the leaders doing differently? Cyber EO champions (leaders who give their agency's EO progress an A) are predictably more likely than their peers to say they have all the funding they need. They are also more likely to have their chief information officer (CIO) leading their zero-trust implementation (67 percent to 28 percent).

When asked for perspectives on what's needed to achieve cyber progress, the research identified the Federal wish list:

- Workforce training and expertise
- Stronger executive buy-in
- Detailed direction from agency IT leadership
- Centers of Excellence (COEs) in the government to lend expertise

Three-fourths of Federal cyber decision-makers also say the EO should have been more authoritative with private-sector directives.

The *Impact Assessment: Cyber EO Year One* report is based on an online survey of more than 150 Federal cybersecurity decision-makers familiar with their agencies' cybersecurity initiatives, including zero trust strategies, in March 2022 and is underwritten by Amazon Web Services (AWS), CrowdStrike, and Zscaler. The report has a margin of error of ±7.7 percent at a 95 percent confidence level.

To review the full findings, including where cyber leaders anticipate the EO will make the most impact in the next five years, and perspectives on the next big issue Federal cyber teams will need to navigate, visit https://www.meritalk.com/study/impact-assessment-cyber-eo-year-one/.

About MeriTalk

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Our award-winning editorial team and world-class events and research staff produces unmatched news, analysis, and insight. The goal: a more efficient, responsive, and citizen-centric government. MeriTalk connects with an audience of 160,000 Federal community contacts. For more information, visit https://www.meritalk.com/ or follow us on Twitter, @MeriTalk. MeriTalk is a 300Brand organization.

# # #

###