



Media Contact:

Logan Prescott

703-883-9000 ext. 145

lprescott@meritalk.com

Operational Technology Cybersecurity Rises as Priority for Federal Agencies – But Gaps Remain

90 Percent of Federal OT Leaders Say Their Agency has Prioritized OT Cybersecurity in the Past Two Years – But Over Half Have Experienced an OT Cyber Incident in the Last Year

ALEXANDRIA, Va. – May 14, 2024 – Sixty eight percent of Federal OT administrators and managers reported experiencing an operational technology (OT) cyber-incident in the past year, and 90 percent have placed greater emphasis on OT cybersecurity. However, only approximately half felt confident they could detect or mitigate a threat today. These insights are contained in a new report from [MeriTalk](#), government IT’s top digital platform, and [Claroty](#), whose mission is to secure the cyber-physical systems of connected organizations. The report identifies critical gaps and cites best practices for Federal security professionals to enhance operational security.

The report, “[Guardians of Government: The State of Federal OT Security](#),” is based on a survey of 100 Federal security administrators and managers overseeing OT in Federal civilian and Department of Defense (DoD) organizations. For this research, OT refers to programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment.

According to the report, only 55 percent of Federal OT leaders felt fully confident they could detect and mitigate a threat if it were to occur today and only 20 percent gave their agency an “A” grade for cybersecurity preparedness. Gaps in network visibility, vulnerability/risk management, and secure remote access and monitoring were all identified as hindering OT security readiness. Additionally, 65 percent are concerned about the number of OT assets in their agency that have reached end-of-life but remain internet facing.

“We are seeing Federal civilian and DoD agencies that place a strategic emphasis on securing their diverse OT environments as among the most prepared to defend against threats to their operations,” commented Heather Young, Regional Vice President, Claroty, U.S. Federal. “These



agencies have prioritized collaboration between OT and IT security teams, they continually assess vulnerabilities, and they are standardizing risk models and upskilling teams to meet current and future threats. This is what is needed to increase resilience across the Federal government.”

One third of respondents cited the complexity of OT environments (including geographic distribution) and the need to increase collaboration between OT and IT security teams as areas for improvement. To accelerate progress, OT leaders recommend standardizing risk models, enhancing visibility and access controls, and upskilling staff.

The report is based on a survey of 100 Federal security administrators and managers conducted in March 2024. The quantitative research has a margin of error of $\pm 9.78\%$ at a 95% confidence level. To view the full findings, [view the report](#).

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 produce 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.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, commercial, and public sector environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City with U.S. federal headquarters in Leesburg, VA. To learn more, visit claroty.com.

###