**FOR IMMEDIATE RELEASE**

Contact:
Amy Pasquarello
703-883-9000 ext. 146
apasquarello@meritalk.com

# FEDERAL ENDPOINT STUDY SHOWS 44 PERCENT OF ENDPOINTS ARE UNPROTECTED OR UNKNOWN; CHANGE IS REQUIRED TO SECURE THIS FRONTIER AND PREPARE FOR INTERNET OF THINGS

*Federal IT Executives Anticipate Progress with CDM Phase II and NIST Framework*

**Alexandria, Va., November 5, 2015** – MeriTalk, a public-private partnership focused on improving the outcomes of government IT, today announced the results of its report, "Endpoint Epidemic." The study, underwritten by Palo Alto Networks, examines the current state of endpoint security across the Federal government, finding 44 percent of endpoints are unknown or unprotected; and that barely half of Federal government survey respondents have taken critical steps to secure endpoints, such as scanning for vulnerable/infected endpoints.

Federal agencies are facing an explosion of endpoints in both volume and variety – providing far more entry points for malicious access into government networks. Today, one-third of Federal IT managers say they have experienced a breach due to APT or zero-day attacks. And, they estimate that 30 percent of their network-connected devices have been infected with some type of malware. Those who seek unauthorized access to government or government employee data can take advantage of the status (known/unknown, secure or insecure) of the first device as a way into sensitive government networks (website launched, document opened, etc.).

In reviewing the proactive steps Feds are taking to prevent, detect, and mitigate endpoint threats, several areas of concern emerged. First, securing the endpoints – 80 percent of Federal IT managers say they don't micro or virtually segment endpoints and 59 percent don't employ real-time patching for high priority vulnerability disclosures. Second, securing the network from unknown files – just 28 percent have identified dubious files from endpoints. Third, ensuring the network is protected contextually by user, application and devices; half of Federal IT managers say their agency

isn't taking key steps to validate users and apps. And, fourth – personal devices; less than half of Federal IT managers say their agency requires employees to register the personal devices they use for work. These same devices are then used for "risky" behaviors such as uploading work documents to a cloud app.

"Endpoints are an increasingly important vector to secure in the cyberattack life cycle," says Pamela Warren, director, government & industry initiatives, Palo Alto Networks. "Unfortunately, these study results indicate that trust and visibility are much too often absent on this frontier. Applying the 'Zero Trust' model from the network to the endpoint with a natively integrated and automated next-generation security platform can dramatically improve visibility and prevent threats to government networks."

Once defined as only servers, desktops, and laptops, endpoints have evolved to include anything connecting to an IT network – from medical devices and ATM machines to military sensors. Despite the growing volume of endpoints, one-third of Federal IT managers say their agency has not updated their formal definition of an endpoint in the past 10 years.

And, with the expansion of endpoints comes the expansion of cyber vulnerabilities – and an even greater need for endpoint security. Sixty-five percent of Fed IT managers believe they need to improve current policies in preventing unknown threats – and also integrate with other security tools (network security, threat intelligence) to get a more comprehensive security view of their network.

When it comes to overall endpoint security policies, 89 percent of Fed IT managers say their agency's policies need to improve – and just over half say their current policies and standards are very effective, practical, or enforceable.

One of the most significant origins of endpoint challenges stem from Federal employees using personal devices for work purposes. Agencies with Bring Your Own Device (BYOD) policies are failing to enforce appropriate policies for those devices among their employees. Forty-five percent of Federal employees who use personal devices for work purposes have either not reviewed their agency's BYOD policy or don't believe one exists.

Even worse, 61 percent of agencies do not apply their network security policies to mobile devices; 52 percent do not enroll devices with the IT department; and 50 percent do not ban the use of public Wi-Fi. Whether it's a lack of restriction or awareness, Federal employees are simply not

protecting agency information – 61 percent of Federal employees who use personal mobile phones for work have downloaded personal applications to that phone. Further, over half admit to risky behavior with personal mobile devices used for work. Thirty-nine percent of Feds email work documents to their personal email accounts or upload them to a cloud application. Thirty percent of Feds have opened an email or text from an unknown contact on the same device used for work. And, 24 percent of Feds say they log into the agency's network using public Wi-Fi at least weekly.

Federal employees say they are willing to cooperate – and even recommend stricter consequences for violating agency BYOD policies. Seventy-nine percent would be willing to have their device inspected for malware. And, 78 percent suggest removing telework privileges for employees that do not comply.

"Telework is terrific – and the Internet of Things promises to change the world as we know it," said Steve O'Keeffe, founder, MeriTalk. "To stay secure, we need to recognize the importance of automation and preventative medicine in cyber security measures – to ensure the health of our government – and the body politic."

Despite the broad impact of endpoint security threats, just 49 percent of IT managers say their agency's endpoint security policies and standards are very well integrated into their overall IT security strategy.

As for other cyber security strategies, 56 percent of Federal IT managers believe the NIST cyber security framework has helped their agency establish a plan for improving current endpoint security measures. And, 80 percent believe CDM Phase II will have a positive impact on their agency's endpoint security.

The "Endpoint Epidemic" report is based on an online survey of 100 U.S. Federal IT managers and 100 Federal employees in September 2015. Each dataset has a margin of error of ±9.78% at a 95% confidence level. Visit www.meritalk.com/endpoint-epidemic to view the full report.

**About MeriTalk**

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Focusing on government's hot-button

issues, MeriTalk hosts Big Data Exchange, Cloud Computing Exchange, Cyber Security Exchange, and Data Center Exchange – platforms dedicated to supporting public-private dialogue and collaboration. MeriTalk connects with an audience of 85,000 government community contacts. For more information, visit www.meritalk.com or follow us on Twitter, @meritalk. MeriTalk is a 300Brand organization.

– 30 –