FOR IMMEDIATE RELEASE

Contact:
Lisa Futterman
703-883-9000 ext. 163
lfutterman@meritalk.com

Cyber Security's Continuous Diagnostics and Mitigation Report Finds Agencies Moving, but Anxious to Pick Up the Pace

Program Goals Require Assessment Cycles to Fall Under 72 Hours; Agencies Call on Information Refreshes Every Day

Alexandria, Va., June 2, 2014 – MeriTalk's Cyber Security Exchange, a public-private partnership focused on improving the outcomes of government IT and cyber security, today announced the results of its new report, "CDM: Under the Hood." Surveying Federal cyber security managers, the study examines the path ahead for the Continuous Diagnostics and Mitigation (CDM) and Information Security Continuous Monitoring (ISCM) program, a government-wide acquisition vehicle established by Department of Homeland Security (DHS) in partnership with General Services Administration. Overall, agencies are moving forward – the overwhelming majority of agencies have met the April 30th and May 30th CDM deadlines. That said, agencies are anxious to pick up the pace, in every way.

While the CDM implementation pace has been impressive thus far, security managers still feel the process is not moving quite fast enough. Fifty-eight percent of respondents believe that the phases of the program are rolling too slowly. In addition, current CDM goals require assessment cycles to fall under 72 hours, but 90 percent of those surveyed want information to be refreshed within 24 hours.

Top Gear

Security managers praised CDM for its benefits – including less operational information security risk of IT systems (56 percent) as well as improved prioritization and risk management (55 percent). While agencies see the opportunity ahead for efficiency in automation, there are hurdles to overcome. Government cyber security managers cite training IT/security staff (56 percent), budget

(55 percent), and difficulty integrating legacy systems (53 percent) as the top barriers to CDM implementation.

Fork in the Road

According to the report, CDM will not change FISMA overnight. Fifty percent still noted a need for FISMA reporting requirements until CDM/ISCM produces adequate data to replace the current system. When asked if their FISMA-compliance budget would change because of CDM, 30 percent said their budget would remain the same, while 26 percent noted that it would increase.

"Based on the report findings, the CDM initiative has grown by leaps and bounds in less than one year," said Steve O'Keeffe, founder, MeriTalk. "So what does this mean for the road ahead? Agencies need greater analytical capabilities, critical application resilience, common trusted identities, and secured shared service environment. Agencies are craving more and want faster delivery of the projects and services available through the program. As we looked under the hood, we have seen that the engine is roaring to life on this important cyber initiative."

The CDM and ISCM program contract serves as a Congressional appropriation to purchase tools and sensors that enhance and expand department and agency ISCM capabilities. "CDM: Under the Hood" is based on an online survey of 152 cyber security professionals in May 2014. In conjunction with the study, MeriTalk interviewed industry CDM partners providing tools and services on the contract. To download the full study, please visit www.meritalk.com/cdm. The study was underwritten by General Dynamics IT, HP, IBM, RedSeal Networks, RSA, Symantec, and Tripwire.

MeriTalk's Cyber Security Exchange (CSX) will continue the discussion on the CDM program on Wednesday, June 18 at the Cyber Security Brainstorm at the Newseum in Washington, D.C. Andrew Onello, Deputy Chief Information Security Officer, Citizenship and Immigration Services; John Streufert, Director, Federal Network Resilience, Department of Homeland Security; and Rod Turk, Director, Office of Cyber Security and Chief Information Security Officer, Department of Commerce will lead a panel session on CDM at the event, followed by sessions on identity management, data breach, and insider threats. The Director for Federal Agency Cybersecurity for The White House, John Banghart, will provide the morning keynote address. For more details and to register, visit www.meritalk.com/cybersecuritybrainstorm.

About MeriTalk's Cyber Security Exchange

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. MeriTalk's Cyber Security Exchange (CSX) is a vertical community of Federal cyber security leaders, project managers, industry, and other government IT community stakeholders focused on public-private collaboration and best-practice exchange. CSX generates operational content, applications, and programs to help the Federal government realize its cyber security goals.

MeriTalk also hosts the Big Data Exchange, Cloud Computing 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.

-30-