FOR IMMEDIATE RELEASE

Contact:
Lindsey Hunter
703-883-9000 ext. 151
lhunter@meritalk.com

Federal Cyber Uncertainty – KVM XYZ Study Showcases Biggest Cyber Threat – Feds Trying to Do Their Jobs

Opportunity to Unleash Productivity with Intuitive, Secure Computer Controls

Alexandria, Va., April 13, 2015 – MeriTalk, a public-private partnership focused on improving the outcomes of government IT, today announced the results of its new report, "Federal Cyber Uncertainty – KVM XYZ," underwritten by Belkin Government. The number of incidents reported by Federal agencies to the Federal information security incident center has increased nearly 680 percent in the past six years.[1] To defend against increasing threats, agencies must comply with various cyber security mandates – CDM, FISMA, HSPD-12, TIC – that often fail to take the user experience into account. As agencies look for ways to enable productivity while ensuring air-tight seals between networks, protecting from both internal and external threats, keyboard-video-mouse (KVM) switching devices may be the answer.

A Growing Threat

Despite Federal agencies' efforts to protect data, cyber threats continue to grow. Between 2009 and 2014, the number of reported breaches on U.S. Federal computer networks rose 73 percent.[2] Sensitive data is pouring out of agencies during these security breaches. In 2014, 1.73 million data records containing bank account information or social security numbers were compromised in 27 government data breaches.[3]

Acronyms to the Rescue?

The Federal mandates around cyber security are an alphabet soup of initiatives designed to protect government data – CDM, FISMA, HSPD 12, and TIC. While agencies have made progress

[1] TechAmerica "CIO/CISO Insights" report
[2] http://www.bostonglobe.com/news/nation/2014/11/10/federal-government-struggles-against-cyberattacks/8ls3WW4Q5baJ9iIO5DPqfM/story.html
[3] http://www.informationweek.com/government/cybersecurity/4-worst-government-data-breaches-of-2014/d/d-id/1318061

against these mandates, and they may be improving cyber security to a degree, Federal managers still lack confidence in their ability to protect sensitive data and experience challenges when it comes to compliance:

- **FISMA:** Just over half of Feds say FISMA has improved security at their agency and only 27 percent were perfectly compliant with FISMA in fall 2013[4]
- **HSPD-12:** Despite all of the PIV cards issued, 5.3 million unprivileged user accounts with limited access can log onto Federal networks with only a user ID and password and 134,287 privileged user accounts – system admins with access to everything – are just using user ID and passwords (instead of PIV)[5]
- **CDM:** Fifty-six percent of Federal agencies are able to measure success in their CDM implementation, but only 44 percent are experiencing better security as a result of the CDM controls[6]
- **TIC:** While successful, TIC is cumbersome for mobile access and reduces easy access to data and apps, one of the major benefits of cloud computing

The Need for KVM Security

Agencies must do more than protect from sophisticated outside cyber threats – they must be just as vigilant against insider threats while ensuring security measures are user friendly. A significant amount of government data resides on endpoints such laptops or other mobile devices – but 66 percent of Feds say they are missing measures for endpoint security management.[7] Nearly half of Federal IT and IT security decision makers say government data is most at risk of breach from employees' or contractors' desktops or laptops.[8] Peripherals (such as a keyboard or mouse) have the ability to both send and receive data, creating a security gap.

"Cyber attacks from within an agency need to be as rigorously addressed as those originating from outside sources," said Mauricio Chacon, Director of Product Development, Belkin Government. "KVM switching devices allow government employees to switch networks with various security levels from one desktop. Agencies need innovative, secure solutions that meet the

[4] MeriTalk, FISMA Fallout: The State of the Union, 2013
[5] http://www.secureidnews.com/news-item/u-s-federal-agencies-lagging-with-piv-strong-authentication/#
[6] SANS Institute's "Continuous Diagnostics and Mitigation : Making it Work"
[7] MeriTalk, The Heart of the Network, 2015
[8] *https://thwack.solarwinds.com/thread/71368*

latest government security standards to protect data from both internal and external threats. Our secure switching solutions are tested to the latest government security standards."

Secure switches eliminate bi-directional data flow and allow for sharing of a single set of peripherals among several computers, while ensuring clear separation between disparate networks. Best practices are emerging that enable government security professionals to address the increasing concern for desktop security through secure KVM solutions, better protecting government data from both internal and external threats. These best practices include monitoring USB ports, avoiding non-secure KVM switches, examining casing and design to ensure the external housing of the switch is tamper proof, and isolating data and the CAC reader.

"Federal cyber security lives in Snowden's and Hillary's shadow," said Steve O'Keeffe, founder, MeriTalk. "KVM spells sounder practical security – liberating the Federal workforce to focus on productivity."

To download the full "Federal Cyber Uncertainty – KVM XYZ" infographic, please visit http://www.meritalk.com/kvm-xyz.php.

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, Data Center Exchange, and Mobile Work 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.

###