



For More Information:

Jim McCubbin, EVP & CFO
WidePoint Corporation
7926 Jones Branch Drive, Suite 520
McLean, VA 22102
(703) 349-2577
jmccubbin@widepoint.com

Brett Maas or David Fore
Hayden IR
(646) 536-7331
brett@haydenir.com

Media Contact:

Meredith Esham
(703) 34902577, ext. 127
mesham@widepoint.com

**WidePoint and SPYRUS Enable Higher Assurance Security for
Microsoft Windows To Go®**

Solution pairing WidePoint digital certificates and SPYRUS WorkSafe live drives addresses security concerns related to “Bring Your Own Device” (BYOD) and business travelers’ mobile computing needs

McLean, Virginia, July 22, 2014—WidePoint Corporation (NYSE Mkt: WYY), a leading provider of Managed Mobility Services (MMS) featuring Cybersecurity and Telecommunications Lifecycle Management (TLM) solutions, announced today its collaboration with SPYRUS, Inc., to issue WidePoint Certificate-on-Device for the SPYRUS WorkSafe and WorkSafe Pro USB 3.0 drives with Windows To Go 8.1 certification, enabling higher assurance security and functionality for mobile workers. The WorkSafe Pro is the only USB 3.0 certified Windows to Go 8.1 drive with XTS-AES 256 hardware encryption and internal FIPS 140-2 Level 3 validated PKI.

With growth in the BYOD trend expected to continue—Gartner predicts that by 2017, half of all employers will require employees to bring their own device (BYOD)—and the increasing demand of workers to use tablets and smartphones for work, government agencies and enterprises alike are trying to balance the need for mobile computing options that keep employees productive with the security needed when employees use personal devices, hotel computers, and other mobile and off-premise means to work.

SPYRUS WorkSafe and WorkSafe Pro drives turn personal computers into compliant enterprise-managed Windows desktops—with or without connectivity. Windows To Go enables a full version of Windows to run from an external USB drive. SPYRUS Windows To Go drives boot the Windows 8 or 8.1 operating environment and completely bypass the host computer’s hard drive. There is no impact on the host computer and no footprint left behind when the drive is shut

down. WorkSafe drives are available in 32, 64, 128GB sizes and currently are the only Windows To Go drives available in 256 GB sizes; with larger size versions planned.

”SPYRUS certified Windows To Go live drives with FIPS 140-2 Level 3 security services, combined with WidePoint digital certificates authorized by the U.S. Government, creates the most secure PC-In-Your-Pocket solution to solve BYOD concerns for the enterprise,” said Tom Dickens, SPYRUS COO. “This all-in-one solution provides strong two-factor authentication services for deployed Windows 7 desktop infrastructures, cloud-based services, or when enterprise users are on travel. There is a significant ROI for the enterprise, with more than 75% savings when compared to purchasing new laptops or tablets for employees or contractors.”

WidePoint Certificate-on-Device digital certificates are being used to provide authentication for WorkSafe or WorkSafe Pro drives and for the owner’s identity, enabling features such as two-factor authentication, smart card logon, secure VPN, encrypted email, digital signatures, and remote revocation of certificates on lost or stolen drives. In addition, by identifying the device, permissions different from those granted to users on their workplace PC can be specified. For example, users may be able to access, but not download, sensitive data when working from a device that does not have hardware-based XTS-AES 256 full disk encryption, as the WorkSafe Pro drive does.

Daniel E. Turissini, WidePoint CTO, said, “The combination of WorkSafe drives and Medium Hardware certificates revolutionizes mobility. WidePoint digital certificates provide not only better security but more convenience for users.” He added, “The WorkSafe drive’s embedded FIPS 140-2 Level 3 encryption plus WidePoint digital certificates provides the high-assurance security needed for employees traveling with their entire PC—and the data and access that comes with it—on a USB flash drive in their pockets.”

“There are more ways to take work mobile than ever before,” said Steve L. Komar, WidePoint CEO & Chairman. “Digital certificates provide security that can keep up with the sophistication of mobile computing capabilities and evolution of devices. WidePoint anticipates increasing adoption in the marketplace of higher assurance using digital certificates as part of our Managed Mobility Service offerings.”

About SPYRUS, Inc.

SPYRUS delivers innovative encryption solutions that offer the strongest protection for data in motion, data at rest and data at work. For over 20 years, SPYRUS has delivered leading hardware-based encryption, authentication, and digital content security products to government, financial, and health care enterprises. To prevent the insertion of untrusted components, patented Secured by SPYRUS™ security technology is proudly designed, engineered, and manufactured in the USA to meet FIPS 140-2 Level 3 standards. SPYRUS has collaborated closely with Microsoft to deliver the first certified hardware encrypted portable platform for Windows 7, Windows 8, and Window 8.1. SPYRUS is headquartered in San Jose, California. See www.spyruswtg.com for more information.

About WidePoint

WidePoint (NYSE Mkt: WYY) is a leading provider of secure, cloud-delivered, enterprise-wide information technology-based solutions that can enable enterprises and agencies to deploy fully compliant IT services in accordance with government-mandated regulations and advanced system requirements. WidePoint has several major government and commercial contracts. For more information, visit www.widepoint.com.

###