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) 349-2577
mesham@widepoint.com

WidePoint Provides Proven Solutions That Can Protect Against Vulnerabilities Such as the OpenSSL 'Heartbleed' Bug

WidePoint solutions using Hardware Security Modules and end-to-end-mutual authentication help mitigate threats like Heartbleed and prepare websites against future, still unknown vulnerabilities

McLean, Virginia – April 17, 2014 – WidePoint Corporation (NYSE Mkt: WYY), a leading provider of secure, cloud-based Managed Mobility Services (MMS) featuring enterprise-wide Telecom Lifecycle Management (TLM) and Cybersecurity solutions, offers comprehensive solutions to protect against online vulnerabilities such as the recently uncovered 'Heartbleed' bug.

WidePoint offers enterprise services and solutions that include effective Hardware Security Module (HSM) implementation and end-to-end mutual authentication to mitigate the impact of yet uncovered vulnerabilities like Heartbleed. Delivered as managed services or an on-premise implementation, these offerings are built on WidePoint's more than twenty years of information assurance and Cybersecurity defense in-depth expertise, including customer training and customer support services that ensure that high assurance solutions are properly designed and implemented to fit enterprise/business needs and assurance levels.

An HSM provides a hardened, tamper-resistant environment to store Private Keys that also supports security best practices, such as ensuring that no single individual can manage those keys, and the protection of those keys in the event of bugs similar to Heartbleed.

The use of "shared secrets" like passwords is another common hacker target that can be extremely costly for consumers and businesses alike. WidePoint CTO Dan Turissini believes that

the time is right for strong digital signature credentials: "It is long past due that cloud-based applications transition away from shared secrets like passwords for authentication. Using strong digital signature credentials can dramatically reduce the impact of vulnerabilities like Heartbleed. Planning and implementation of measures beyond simply patching OpenSSL are essential."

"WidePoint customers can rely on the security of our solutions," said Steve L. Komar, WidePoint CEO & Chairman. "WidePoint's trusted environment can be leveraged to secure and archive SSL Private Keys, and more importantly, our expertise can be leveraged by our enterprise PKI customers to ensure they have the most comprehensive and functionally redundant Cybersecurity solutions to avoid catastrophic financial and liability impact that could occur with the next 'Heartbleed'."

More information on Heartbleed can be found here: http://heartbleed.com

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.

###