Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL INVITES PAYMENTS COMMUNITY TO INPUT ON PIN TRANSACTION SECURITY

Feedback period for Hardware Security Module (HSM) security requirements now open to PCI Participating Organizations

WAKEFIELD, Mass., February 07, 2012 —The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today announced the launch of a 30-day period to solicit feedback from PCI Participating Organizations on the next version of the PCI Hardware Security Module (HSM) security requirements. PCI stakeholders have until Friday March 09, 2012, to provide their input on these requirements designed to secure cardholder data in all point-of-sale environments.

To develop and maintain strong technical standards and resources for the protection of payment card data, the PCI Council relies heavily on feedback from its Participating Organizations, including more than 630 of the world’s leading merchants, financial institutions and technology and service providers.

Hardware security modules (HSM) are non-cardholder facing devices used in connection with the protection of sensitive data, such as cardholder data (e.g. PINs), and the cryptographic keys that protect or authenticate that information. For example, HSMs are used with PIN translation, payment card personalization, data protection and e-commerce. Requirements for testing and approving these devices fall under the PCI PIN Transaction Security (PTS) program that also tests and validates Point of Interaction (POI) devices to ensure they comply with industry standards for securing sensitive data.

—more—

As part of a regular lifecycle for updating these requirements, the Council has made a number of modifications to version 1.0 aimed at providing greater alignment between the PCI Hardware Security Module (HSM) security requirements and those introduced with version 3 of the PTS Point of Interaction (POI) security requirements.

The Council requests input from Participating Organizations on these changes. All feedback will be reviewed and considered in finalizing the revised requirements for publication in the spring. Organizations should submit feedback using the online tool at https://programs.pcissc.org/.by March 09, 2012.

Also, Participating Organizations and assessors have the opportunity to participate in the formal feedback period for the PCI DSS and PA-DSS, which is open until the end of March at https://programs.pcissc.org/. Please email support@pcisecuritystandards.org for assistance with credentials or with any questions on using the feedback tool.

“Because the Council is comprised of organizations ranging from merchants to acquirers to processors we have a unique opportunity to create standards based on feedback from across the payments spectrum. We rely heavily on active participation by our members. This industry feedback and expertise is critical to our mission and our business,” said Bob Russo, general manager, PCI Security Standards Council. “I would like to encourage each organization to take the time to provide us with input during this period.”

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###