Media Contacts

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

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL RELEASES SUMMARY OF FEEDBACK ON PCI STANDARDS

—Global industry input drives updates to the next version of the PCI Standards to be released in 2013—

WAKEFIELD, Mass., September 05, 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 released a summary of feedback from the PCI community on the PCI Security Standards. The document highlights key themes coming out of the Council's formal feedback period on version 2.0 of the PCI DSS and PA-DSS, in preparation for the next release of the standards in October 2013.

As part of the open standards development process for the PCI DSS and PA-DSS, the PCI Security Standards Council (PCI SSC) solicits input on the standards from its global stakeholders through a variety of avenues, including a formal feedback period. More than half the input received during the formal feedback period originated from organizations outside of the United States.

This industry feedback drives the ongoing development of strong technical standards for the protection of cardholder data, providing more than 650 Participating Organizations, including merchants, banks, processors, hardware and software developers, Board of Advisors, point-of-sale vendors, and the assessment community the opportunity to play an active role in the improvement of global payment security. Payment security stakeholders can use the summary document to better understand the Council's approach to reviewing and categorizing the feedback, key trends and themes, and how the feedback is being addressed.

—more—

The feedback was received by the Council across the following five categories: request change to existing requirement/testing procedures (34%); request for clarification (27%); request for additional guidance (19%); feedback only – no change requested (12%); and request for new requirement/testing procedure (7%). Over 90 percent of the feedback was on the PCI DSS, the foundation for the Council's standards, with more than half specific to the following topics:

- **PCI DSS Requirement 11.2** – Suggestions include prescribing use of specific tools, requiring ASVs to perform internal scans, and defining what constitutes a "significant change".
- **PCI DSS Scope of Assessment** – Suggestions for detailed guidance on scoping and segmentation.
- **PCI DSS Requirement 12.8** – Suggestions include clarifying the terms "service provider" and "shared," and providing more prescriptive requirements regarding written agreements that apply to service providers.
- **PCI DSS SAQs** – Suggestions for updating the SAQs; they are either too complex or not detailed enough.
- **PCI DSS Requirement 3.4** – Suggestions for further clarification and guidance since encryption and key management are complex requirements, and truncation/hashing & tokenization is not a convenient method to store and retrieve data
- **PCI DSS Requirement 8.5** - Suggestions for updating password requirements, including expanding authentication beyond just passwords; current password requirements are either too strict or not strict enough, be either less prescriptive or more prescriptive.

These trends and other highlights are provided in the summary document, including main PA-DSS feedback themes, breakdowns of the types of organizations that participated and geographic regions represented.

As a benefit of involvement in the PCI community, a more detailed version - including all feedback comments received and how the Council initially proposes to address these items is available for Participating Organizations and assessors on the PCI PO portal. Discussion of this feedback will be a primary focus at the Council's 2012 Community Meetings in Orlando, Florida on September 12-14 and Dublin, Ireland on October 22-24.

Following the Community Meeting, as part of the next phase of the development process, the Council will begin drafting the updated standards based on stakeholder input and additional research and analysis. Full details on the standards development

lifecycle can be found here: https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf.

“Industry feedback is the lifeblood of the PCI Standards,” said Bob Russo, general manager, PCI Security Standards Council. “As the PCI community continues to expand across industries and geographies, the Council relies on its expertise to drive the evolution of the standards. I want to personally thank all who have contributed to the ongoing development of these critical resources for payment security.”

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

###