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 ANNOUNCES UPDATE TO POINT-TO-POINT ENCRYPTION PROGRAM

- *With updated criteria, testing procedures and training for validating hardware-based P2PE solutions Council continues focus on technologies that help reduce PCI DSS scope for merchants -*

WAKEFIELD, Mass., April 27, 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 availability of updated requirements for point-to-point encryption (P2PE) solution providers to implement hardware- based solutions for merchants to use, including testing procedures and training for assessing these solutions.

The Council first introduced its point-to-point encryption program at the end of 2011. The initial requirements set the standard for hardware-based point-to-point encryption solutions, providing a method for vendors to validate their P2PE solutions and for merchants to reduce the scope of their PCI DSS assessments by using a validated P2PE solution for accepting and processing payment card data.

Today's release of *Point-to-Point Encryption: Solution Requirements and Testing Procedures – Encryption, Decryption, and Key Management within Secure Cryptographic Devices* builds on the initial requirements to provide clarification, additional guidance and program information including:

- A new section to incorporate merchant-focused guidance for use of a validated P2PE solution
- Scope of assessment for P2PE solutions
- Guidance on scenarios where there are multiple acquirers involved with a single solution

—more—

A summary of these changes is included as a separate document to help solution providers easily identify where the requirements have been updated and perform a gap analysis accordingly. Additionally, for assessors evaluating P2PE solutions, the document contains detailed steps on how to test and verify that a specific requirement is in place.

As part of the program, the Council has also introduced training for assessors to help them understand how to use these testing procedures in the context of a P2PE solution review. The in-depth program offers eligible security companies the opportunity to become Qualified Security Assessors (QSA (P2PEs)) and Payment Application Qualified Security Assessors (PA-QSA (P2PEs)) to enable them to assess compliance to the PCI P2PE standard. The 3-day instructor-led session covers all the components of the P2PE requirements and program including terminology, roles and responsibilities and reporting, and detailed information about the testing procedures. Currently scheduled sessions include:

- May 11-13, 2012
  Denver, Colorado
- June 25-27, 2012
  Manchester, England, UK

Interested companies should consult the *P2PE QSA Qualification Requirements* to determine eligibility. For more information or to register for a training session, please visit: https://www.pcisecuritystandards.org/training/p2pe_training.php

Once assessors are trained and solutions have been validated and accepted, the Council will provide a listing of validated solutions on the PCI SSC website that merchants can use to choose a secure solution. Eligible merchants using these solutions will be able to validate to a reduced set of PCI DSS requirements. To help with this validation process, the Council is working to develop a new Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC), which will be released later this spring along with the P2PE program guide for use by P2PE assessors and P2PE solution providers.

In the meantime, the Council encourages merchants to review the section titled "Merchants Using P2PE Solutions" in these solution requirements to better understand P2PE and PCI DSS scope, but reminds organizations that these do not supersede the PCI Data Security Standard, nor is a merchant mandated to use P2PE technology.

"The PCI P2PE program provides a means for solution providers to meet many of the merchant's PCI DSS requirements on behalf of the merchant," said Bob Russo, general manager, PCI Security Standards Council. "With these updated P2PE requirements and program in place to assess and validate these solutions securely, we're one step closer to helping merchants take advantage of this technology to simplify PCI DSS validation efforts and mitigate potential breaches."

The next phase of the point-to-point encryption program this year will focus on requirements for solutions that combine hardware based encryption and decryption through secure cryptographic devices, with software that may manage transaction-level cryptographic keys for decryption. The Council also will continue to explore the development of requirements for software solutions that encrypt cardholder data at the point of merchant acceptance, and/or decrypt cardholder data at a host system.

Point-to-point encryption will be a key topic of discussion at the Council's Annual Community Meetings scheduled for September 12-14 in Orlando, Florida and October 22-24 in Dublin, Ireland. For more information, please visit: https://www.pcisecuritystandards.org/communitymeeting/2012/.

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 related 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: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linked-in.com/company/pci-security-standards-council

Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###