

PRESS RELEASE



Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Media Contacts

Glenn R. Boyet	Ella Nevill or Matthew Mors
PCI Security Standards Council	Text 100 Public Relations
+1 (781) 876-6248	+1 (617) 399-4915 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	pci@text100.com

PCI SECURITY STANDARDS COUNCIL ISSUES LATEST PIN ENTRY DEVICE REQUIREMENTS DRAFT FOR COMMENT AND REVIEW

—Unattended payment terminals and hardware security modules added to the PED Security Requirements; Participating Organizations to provide input and review—

WAKEFIELD, Mass, August 4, 2008 — The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announced availability of the draft requirements for unattended payment terminals (UPTs) and hardware (or host) security modules (HSMs) under the PED program. The availability of this draft, now out for comment, is restricted to Participating Organizations in the Council.

The Council recently [announced](#) the addition of UPTs and HSMs under the PED Security Requirements in an effort ensure that these hardware devices will now undergo a rigorous testing and approval program to ensure they comply with industry standards for securing sensitive cardholder account data during any point in the transaction process. When fully implemented after the review period and final distribution of the revised requirements, the Council will maintain the list of approved UPTs and HSMs, provide documentation and training for labs evaluating these devices and be the single source of information for device vendors and their customers.

Participating Organizations will have until September 30, 2008 to provide feedback and comment on the draft additions. This feedback will be collected and analyzed by the Council with the intention of delivering the final updates by end of 2008. This process is the standard feedback mechanism applied by the Council for all of the standards it manages.

“It is the Council’s continued mission not only to protect cardholder account data and all aspects of the payment card transaction process, but to also ensure that our standards include the input of stakeholders,” said Bob Russo, General Manager, PCI Security Standards Council. “Providing our participating organizations with the opportunity to comment on revisions and additions to our standards ensures we meet this goal.”

For More Information:

—more—

More information on the PCI Security Standards Council and becoming a Participating Organization please visit pcisecuritystandards.org, or contact the PCI Security Standards Council at participation@pcisecuritystandards.org. For more information on the latest in PED Security Requirements visit

http://www.pcisecuritystandards.org/security_standards/ped/index.shtml.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors and other vendors are encouraged to join as Participating Organizations.

###