Payment Card Industry
Security Standards Council, LLC

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

PCI SSC bulletin on impending revisions to PCI DSS, PA-DSS

13 February 2015

To ensure the continued strength and integrity of PCI Standards for payment data protection, the Council has ongoing processes for monitoring threats and vulnerabilities and for updating the standards as necessary. The National Institute of Standards and Technology (NIST) has identified the Secure Socket Layers (SSL) v3.0 protocol (a cryptographic protocol designed to provide secure communications over a computer network) as no longer being acceptable for protection of data due to inherent weaknesses within the protocol. Because of these weaknesses, no version of SSL meets PCI SSC's definition of "strong cryptography," and revisions to the PCI Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS) are necessary.

After working with stakeholders over the last several months to understand the impact to the industry, the Council will soon publish PCI DSS v3.1 and PA-DSS v3.1 to address this issue and provide other minor updates and clarifications.

When published, PCI DSS v3.1 will be effective immediately, but impacted requirements will be future-dated to allow organizations time to implement the changes. For PA-DSS v3.1, the Council is also looking at how to address both future submissions and currently listed applications. A summary of changes document for each standard and FAQs will accompany the release of the revised standards to help clarify the impact of these changes.

In the interim, as there is no known way to remediate vulnerabilities inherent in the SSL protocol, the PCI Security Standards Council urges organizations to work with your IT departments and/or partners to understand if you are using SSL and determine available options for upgrading to a strong cryptographic protocol as soon as possible.

Additional Resources
Further details are provided in the following:

- NIST SP 800-57: Recommendation for Key Management – Part 1: General (Revision 3)
- NIST SP 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (Revision 1)