

White Paper: PCI DSS v1.2 Release Update Notes

By:

**Christopher S. Harper
Vice President of Technical Services
Secure Enterprise Computing, Inc**

October 29, 2008



NOTE CONCERNING INTELLECTUAL PROPERTY AND SOLUTIONS OF SECURE ENTERPRISE COMPUTING, INC.

Copyright © 2008 By Secure Enterprise Computing, Inc. All Rights Reserved.

Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Secure Enterprise Computing, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Secure Enterprise Computing's Inc. research may discuss legal and/or compliance issues related to the information technology business, Secure Enterprise Computing, Inc. does not provide legal advice or services and its research should not be construed or used as such. Secure Enterprise Computing, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.



White Paper: PCI DSS v1.2 Release Update Notes

Christopher S. Harper, Vice President of Technical Services, Secure Enterprise Computing, Inc.

Since the updated Payment Card Industry Data Security Standard (PCI DSS) was released on October 1, 2008, we have had many questions regarding changes to the standard and how they may impact an organization's compliance efforts.

As technical team lead at Secure Enterprise Computing, I was fortunate enough to attend the recent PCI Security Standards Council Community Meeting held the week prior to the version 1.2 release. The updated standard was discussed in depth as well as other topics related to the security of credit card data. The community meeting was a unique opportunity to engage directly with the council's Technical Working Group which is responsible for ongoing development of the PCI DSS.

In this overview, I will discuss the changes and updates to the standard as well as highlight some of the topics that arose during the panel discussions.

Highlights from PCI Security Standards Council Meeting in Orlando

Overwhelmingly, the changes to the standard involve clarification of the prior standard to address many of the concerns that merchants, service providers and others had. It is also an attempt to incorporate current best practices and address emerging risks and threats to the security of credit card data. Version 1.2 is not a rewrite of the standard, nor will anyone have to retool their PCI compliance efforts.

The new version has also combined documentation that was previously separate from the standard into the standard itself. A single document download will now provide information about reaching compliance such as scoping your cardholder environment, network segmentation (a little about that topic later in this document), the applicability of the standard to wireless networks, reporting guidelines, and some guidance on selecting representative samples when assessing your network for compliance.

During the sessions with the Technical Working Group, the topic most often raised was that of network segmentation. Using network segmentation to effectively reduce the scope of the cardholder environment is an area where a merchant can reduce the scope of devices or systems which must be kept in compliance, thereby reducing the overall costs and effort involved with reaching compliance. Careful judgment and sound security practices should be employed when reaching this goal. While isolation of the cardholder environment can reduce risk due to the protection used to achieve isolation, you must first have a thorough understanding of how cardholder data flows through the environment. This is essential to isolating the cardholder environment. Each network is unique, but here are a few rules of thumb with respect to network segmentation:

- The segmentation that would separate the cardholder data environment from the rest of the "out of scope" network should be a true network firewall product or a router with "strong ACLs".
- When assessing whether network segmentation is adequate, you should be able to truly verify that the cardholder environment is isolated (at the network layer).
- If you are separating an out-of-scope wireless network, a network firewall should be used. In-scope wireless networks (those used to store, process, or transmit cardholder data) must adhere to the applicable standards such as 1.2.3, 2.1.1, and 4.1.1.

An interesting example was given whereby a workstation from the out of scope network traverses the firewall to access the in-scope network using a Secure Sockets Layer (SSL) connection. The TWG concurred that this workstation would be considered within the scope of the cardholder environment. The group was careful however, not to give specific advice regarding individual scenarios, due to the complexity and uniqueness of each environment.

With regard to segmentation and scope, I caution everyone that a breach of cardholder data whether via an in-scope host or not would still have the same ramifications. "A breach is a breach."

The new version of the PCI Data Security Standard has an added section that addresses network segmentation and covers the subject in general terms. It is important to understand however, that segmenting the network is not a requirement of the PCI DSS.

It was also interesting to hear the group respond to questions regarding sampling of systems and components in an assessment situation. Sampling can be used to reduce the amount of work required to determine the state of compliance. The overwhelming view of the council in this regard is that the sample group can be sized in accordance with the level of standardization in the environment. The more comprehensive the standards are that dictate how systems, sites or environments are built, configured and maintained, the smaller the sample group can be. They also stressed that the approach that was taken to sampling should be well documented. Again, good judgment is crucial.

Specific Changes to the PCI DSS

Below is a section-by-section overview of the significant changes and what they may mean in terms of your compliance efforts. I haven't addressed every minute change, but I do address the most significant changes relevant to the challenges we have seen merchants face in the past.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 1 clarifies that the requirement applies to both firewalls and routers. The business justification for ports, protocols and services has been combined into a single sub-requirement. The term "risky" which was used to describe protocols such as Telnet or FTP has been changed to insecure. The council has also removed Requirement 1.1.9 which referenced configuration standards for routers. Finally, the new standard combines some of the sub-requirements and there is a note defining an "untrusted network."

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

With respect to securing wireless environments, the standard now specifies that it applies to Wi-Fi networks that are "connected to the cardholder data environment or transmitting cardholder data." References to specific technologies such as WEP have been removed from the standard and the requirement to disable SSID broadcasts has been removed, since it is trivial from an attack standpoint to obtain the SSID. The WPA / WPA2 requirement has been changed to require that firmware exist that supports these technologies. Requirement 2.4 specifies that it is intended for "shared hosting providers" and that they must adhere to *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*.

Requirement 3: Protect stored cardholder data

The majority of Requirement 3 involves replacing terms or making terms consistent throughout the requirement. Since much of Requirement 3 involves the encryption of data at rest (i.e., in storage, such as in a database), many of the terminology updates relate to encryption.

Primary Account Number (PAN) is used consistently instead of "data," "credit card data," or "cardholder data". "Strong Cryptography" and "cryptographic" are used in place of "encryption" and a definition of strong cryptography is given in the glossary or terms.

References to different types of logs have been changed to "all logs" and examples are given, such as transaction or debugging logs.

Many of the remaining changes to Requirement 3 involve minor clarifications and the combining of sub-requirements.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

New implementations of WEP are not allowed after March 31, 2009. Furthermore, the use of existing WEP implementations must be discontinued after June 2010. This is an obvious recognition that WEP is no longer considered safe technology.

Sub-requirement 4.2 has been changed from referencing "email" and now states "end user messaging technologies" such as email, instant messaging, and chat protocols.

Requirement 5: Use and regularly update anti-virus software and programs

Version 1.1 of the standard all but excluded Unix and mainframe systems from the A/V requirement by stating that they were not commonly prone to virus attacks. The new standard has been amended to remove these exceptions. The intent of this requirement remains the same in that, where applicable technologies exist, anti-virus software should be installed and properly configured on all system components commonly affected by malicious software. Anti-virus logs must also be handled in accordance with Requirement 10.7 which specifies log retention times.

Requirement 6: Develop and maintain secure systems and applications

Requirement 6 has changed the patch deployment requirement so that merchants can now take a risk-based approach. Higher risk systems and components should be patched within one month, where lower risk systems can be patched within three months.

The code review requirements have been clarified to state that it applies to all custom code. Internal parties can perform the code reviews but should be performed by someone other than the author, and management review and approval should be involved. Additional references have been added with respect to the Open Web Application Security Project (OWASP).

The June 2008 best practice of either performing code reviews or installing a Web Application Firewall (WAF) is now a requirement. Clarifications which have existed since February 2008 in the *Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified* document have also been worked into the standard.

The technical working group stated that meeting the “review public-facing web applications” option of 6.6 was not a code review requirement. Rather, it should be seen as a workable replacement of the WAF functionality which was to at least protect the application from the OWASP Top Ten categories of vulnerabilities. The “review” option should be seen as an application-layer vulnerability assessment. It should be done at least annually and after changes to the application have been made.

The other option available with respect to meeting Requirement 6.6 is to install a Web Application Firewall (referred to in the 1.1 standard as an application layer firewall). These are typically appliance-based solutions that are specifically designed to protect a web environment against common and emerging attacks against the application itself.

Requirement 7: Restrict access to cardholder data by business need to know

Very few changes have been made to Requirement 7. The new standard defines “need to know” as “when access rights are granted to only the least amount of data and privileges needed to perform a job”. Other changes include text to clarify the intent such as “computing resources and cardholder information” being changed to “system components and cardholder data.”

Requirement 8: Assign a unique ID to each person with computer access

References to remote access in Requirement 8 pertain to remote access to the systems involved with the storage, processing and transmission of cardholder data. 8.3 defines remote access as “network-level access originating from outside the network.”

Other changes have been made for consistency and clarification, such as the changes from “encrypt all passwords” to “render all passwords unreadable” in 8.4 and “inactivated” to “deactivated,” “remove” to “remove or disable,” and “inactive” to “disabled” in 8.5.4, 8.5.5, and 8.5.6 respectively.

They stress that all access to cardholder databases should be authenticated and that direct access to the database should be restricted to database administrators and applications.

Requirement 9: Restrict physical access to cardholder data

Item 9.1.1 has been changed from requiring the use of cameras to “cameras or other access control mechanisms” to monitor access to sensitive areas. “Sensitive areas” has been defined as “any data center, server room or any area that houses systems that store, process, or transmit cardholder data.”

9.2 has added “contractor” to the description of an employee. The intent is that a full- or part-time individual would be distinguishable from a visitor. 9.5 has been modified such that offsite storage facilities (where secure media backups are stored) should be visited at least annually. 9.6 is now clarified to apply to paper and electronic media that contain cardholder data.

Requirement 10: Track and monitor all access to network resources and cardholder data

The issue of collecting log data centrally and subsequently being able to derive valuable security data from this log data is something that many organizations struggle with. Being able to “review logs daily” is almost impossible, even in an environment where a small number of systems exist in the cardholder environment.

The council now states in 10.7 that this data should be “immediately available for analysis,” further making the case for the use of an automated tool to perform the log reviews.

10.5.4 has been clarified such that external-facing technologies should write logs onto an internal log server. This is so that, in the event of a compromise of one of these systems, sensitive log data would not be retained on the local system.

Requirement 11: Regularly test security systems and processes

The new standard has added the use of wireless analyzers or wireless IDS/IPS to identify all wireless devices. It has always been the intent that a merchant test for the existence of unauthorized wireless devices, whether the organization officially uses wireless or not.

11.2 and 11.3 have been clarified somewhat, both in the standard and via the supporting documents found on the PCI Security Standards Council website. Penetration testing, which goes quite a bit further than vulnerability testing, must be performed both on internal and external networks and at both the network layer and the application layer. The new standard clarifies that these tests do not have to be performed by a QSA or ASV, but must be performed by a qualified third party or someone from the organization who can demonstrate independence from the systems being tested.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

In addition to several terminology changes, 12.3 has been expanded to include additional examples of remote access technologies. It has also been clarified that ‘copy,’ ‘move’ and ‘paste’ functions are prohibited while using remote access technologies.

To comply with 12.6, an organization must now require employees to acknowledge, at least annually, that they have read and understood the security policy.

12.8 and 12.10 have been combined to provide more clarity regarding policy and procedures that apply to data shared with service providers.

Finally, 12.9, which addresses the incident response plan, has been updated to make the requirements and testing procedures more consistent.

Several other changes have been made in how the PCI DSS is presented and documented. Appendices now exist to help with the Reports on Compliance and Scoping and Sampling. Overall, the new 1.2 version is an update to the previous version that addresses many of the questions and concerns merchants have raised with the council over the past two years. It also addresses the changing technology and threat climate.

Secure Enterprise Computing is happy to answer any questions you may have regarding the PCI Standard and how it may impact your organization. Please feel free to contact any of us at any time.



Secure Enterprise Computing, Inc.
909 Aviation Parkway, Ste 600
Morrisville, NC 27560

p: 919.380.7979
f: 919.380.9055
e: info@secure-enterprise.com

Sales

Randall Bennett rbennett@secure-enterprise.com
Laurie Leigh lleigh@secure-enterprise.com

Technical

Chris Harper charper@secure-enterprise.com