



November 29, 2006

The PCI Security Standards Council recently published a revised version of the Payment Card Industry Data Security Standard (PCI DSS). The standard is comprised of 12 Requirements for securing cardholder and sensitive authentication data.

With the release of this new version, the PCI DSS Requirement 2 now specifically points users to the Center for Internet Security Benchmarks in support of sub-requirement 2.2 for configuration standards.

"2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)."

In addition, PCI DSS includes other requirements for which the CIS Benchmark configuration recommendations are useful for achieving PCI DSS compliance:

- 1.1 - Firewall configuration;
- 1.1.9 - Router configuration;
- 6.3.1 - Patch deployment; and
- 6.4 - Change control.

The revised PCI DSS can be found at https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.