SecureState
Your Security Team

February 23, 2012

To Whom It May Concern,

SecureState, a qualified QSA company, reviewed *Cisco's Virtual Multi-Tenant Architecture (VMDC) version 2.2*, with regard to its ability to be configured in compliance with PCI-DSS v2.0 requirements. SecureState reviewed all 12 PCI-DSS requirements which are listed below:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for personnel

Keeping in mind that the client has the overall responsibility to ensure PCI compliance, SecureState performed a Gap Assessment against Cisco's VMDC Architecture to ensure it could facilitate PCI compliance. The Assessment was made on an architecture that included both virtual and physical servers. Within this architecture, Cisco's Virtual Security Gateway virtual firewall was evaluated and its functionality was reviewed. Through this Assessment, it was determined that Cisco's VMDC architecture *can* be configured in a PCI compliant manner. In addition, this architecture has the ability to be configured in a manner which can sufficiently reduce PCI scope.

SecureState has worked with Cisco to provide a PCI Deployment Supplemental Guide to this solution. This guide provides guidance as to how to effectively segment the Cardholder Data Environment as well as references and links as to how to configure network components in a PCI compliant manner.

* Following steps outlined in the PCI Supplemental Guide alone does not guarantee PCI compliance. The client still needs to perform their own assessment to better understand client PCI obligations.

Sincerely,

Andrew Weidenhamer, QSA, PA-QSA, CISA, CISSP, CIPP
SecureState
216.927.8200