



Securing Citizen Payment Card Data At-A-Glance

Cisco PCI Solution for Government: Securing Citizen Payment Card Data

Government organizations face growing threats to their citizen's financial data from sophisticated, malicious attacks on their information systems. Complying with the Payment Card Industry Data Security Standard (PCI DSS) can be a daunting task for any organization. The Cisco® PCI Solution for Government helps government retailers and agencies use their existing network to simplify the PCI compliance process.

The Payment Card Industry Standard

The PCI DSS applies to all organizations, public and private, that process, transmit, or store credit card transactions and citizen information. PCI DSS, effective January 1, 2011, includes clarifications designed to make it easier for agencies to address requirements:

- Reinforcement of the need to thoroughly scope data storage and network infrastructure environments.
- Promoting more effective log management in securing cardholder data.
- Allowing a risk-based approach based on specific business circumstances in order to assess and prioritize vulnerabilities.
- Better accommodation for the unique environments of smaller agencies, helping to simplify their compliance efforts.

PCI Enforcement Guidelines

Each financial institution or payment card brand determines its own compliance validation levels. Only the acquiring financial institution can assign a validation level to government merchants and agencies.

Links to card-brand compliance programs include:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp
- Visa Europe: www.visaeurope.com/ais

Individual payment brands also enforce merchant compliance, and fines can range from US\$5,000 to \$500,000. Fines can also be accompanied by ongoing monthly penalties, additional fines per breached record, and possible cancellation of an agency or government retailer's credit card service privileges for continued noncompliance. In addition to the penalties for noncompliance, a credit card breach can cost your agency exponential amounts in possible litigation from card holders, legal fees, and damaged reputation for the agency and elected officials.

Simplifying Compliance: Cisco Solution for PCI

The Cisco Solution for PCI is built on network security best practices, proven Cisco products, Cisco Services, and partner technologies that are validated for compatibility with Cisco PCI Solution for Government architectures and meet Payment Card Industry standards. Because PCI covers many parts of the network, no single product or technology meets all PCI technology requirements.

Cisco and Partner Products with PCI Intelligence

Many Cisco products already include features and the specific intelligence needed to help meet PCI requirements:

- Routing: Cisco Integrated Services Routers (ISR, ISR G2), Cisco Aggregation Services Routers (ASR).
- Switching: Cisco Catalyst® compact switches, Cisco Catalyst access switches, and Cisco Catalyst data center switches, Cisco Nexus® 1000V Series Switches, Cisco Nexus 5000 and 7000 Series Switches, Cisco Application Control Engine (ACE), Cisco Multilayer Director Switch (MDS) with Storage Media Encryption module.
- Network Security: Cisco Adaptive Security Appliance (ASA), Cisco IronPort® Email Security Appliance, Cisco Network Admission Control (NAC) Appliance, Cisco AnyConnect™ VPN, Cisco Firewall Services Modules (FWSM), Cisco Intrusion Detection System Services Modules (IDSM), Cisco Intrusion Prevention System Appliances (IPS), Cisco Nexus Virtual Security Gateway (VSG), Cisco IOS® Firewall, Cisco IOS IPS, Cisco Secure Access Control Server (ACS).

- **Wireless:** Cisco Aironet® Access Points, Cisco Wireless LAN Controllers, Cisco Mobility Services Engine with Enhanced Local Mode (ELM), Cisco Adaptive Wireless IPS.
- **Physical Security:** Cisco Video Surveillance Operations Manager (VSOM), Cisco Video Surveillance IP Cameras, Cisco Physical Security Multiservices Platform (MSP), Cisco Physical Access Manager, Cisco Physical Access Gateways.
- **Compute Systems and Storage:** Cisco Unified Computing System™ (UCS), Cisco UCS Express.
- **Management:** Cisco Security Manager, Cisco Wireless Control System (WCS), CiscoWorks LAN Management Solution (LMS).
- **Voice:** Cisco Unified Communications Manager, Cisco Unified IP Phones.
- **WAN Optimization:** Cisco Wide Area Application Engine (WAE), Cisco Wide Area Application Services (WAAS).



Government Architecture Built on Validated Design

A critical element of the Cisco PCI Solution for Government is Cisco network architecture and validated network designs. Cisco network architectures have been designed for government facilities, data centers, contact centers, and the Internet edge to support e-commerce operations, store employees, citizens, and teleworkers. Cisco PCI Solution for Government also supports wireless 3G technology deployments and multiple formats, including kiosks and stores, in addition to typical small, medium, and large facilities. Cisco network architectures include solutions for virtualized, wired, and wireless deployments. Built and tested in Cisco labs, these designs have been audited by a PCI Qualified Security Assessor, who then provided a assessment report outlining how each solution addresses PCI DSS technology requirements. Cisco Validated Designs for PCI can be downloaded from www.cisco.com/go/govpci

Validated Technology Partners

Products from Cisco technology partners have been validated for compatibility with Cisco PCI Solution for Government network designs and products. Technology partners include:

RSA: Authentication, security, and compliance technology for data centers and stores. Products include:

- **RSA Archer eGRC Platform:** An integrated governance, risk, and compliance platform that helps agencies assess security, identify areas of concern, prepare for a PCI audit and manage the reporting process.
- **RSA enVision®:** Tightly integrated with RSA Archer, RSA enVision offers an effective security and information event management (SIEM) and log management system, capable of collecting and analyzing large amounts of log and event data in real-time.
- **RSA SecurID®:** Two-factor authentication based on something you know (a password or PIN) and something you have (an authenticator); provides a much more reliable level of user authentication to cardholder data than reusable passwords.
- **RSA Data Loss Prevention (DLP) Suite:** Enables organizations to discover and classify cardholder data, educate end users and ensure cardholder data is handled appropriately, and report on risk reduction and progress towards policy objectives.
- **RSA Data Protection Manager:** Enterprise tokenization and encryption controls further strengthen PCI compliance by protecting cardholder data at rest and in transit across public networks.

VCE: Next-generation virtualized converged infrastructure and private cloud technology

- **Vblock™ Infrastructure Platforms:** Pre-integrated, best-in-class datacenter infrastructure and rapid deployment private cloud platforms. Built with industry-leading VMware virtualization; Cisco networking and computing; and EMC storage, security, and management technologies.

HyTrust: Virtualization infrastructure security and logging

- **HyTrust Appliance:** Policy management, access control, logging, and logical infrastructure segmentation for virtual infrastructures.

EMC: Storage and storage management technology. Products include:

- **EMC CLARiiON CX4 Series Storage Area Network (SAN):** Scalable networked storage optimized for virtualized environments.
- **EMC Ionix™ Unified Infrastructure Manager (UIM):** Simplified, integrated provisioning, configuration, change, and compliance management across network, storage, and compute resources for Vblock Infrastructure Platforms.

- EMC Ionix™ Network Configuration Manager (NCM): Model-based and automated compliance, change, and configuration management for networks.

Verizon Business: Consulting Services

- Qualified Security Assessor: PCI audit, PCI readiness assessments, PCI Compliance Management Program, penetration testing, vulnerability scanning, and PCI consulting and remediation services.

The Benefits of the Cisco Solution for PCI

The Cisco Solution for PCI addresses many of the 12 PCI DSS requirements and helps government agencies simplify their compliance strategies. It goes beyond just the requirements to provide comprehensive best practices for securing sensitive citizen information. In addition, the Cisco PCI Solution for Government helps you protect contact center information, mobile applications and data. It helps you build a foundation for ongoing compliance, enhance your agency's physical security and risk management, strengthen citizen data security, and enable new initiatives to serve your communities.



Why Cisco?

Whether you have a single location or hundreds of locations, Cisco has the solutions, experience, and expertise to help improve your effectiveness and operational capacity. The Cisco PCI Solution for Government helps you pull everything together to effectively address the PCI Data Security Standard.

Learn More Today

For more information on the Cisco PCI Solution for Government, visit <http://www.cisco.com/go/govpci>