



The PCI Security Standards Council

Andy Fulton
November 2011



Agenda

About the Council

What is being Protected?

The PCI Standards

Council Resources



About the Council

Open, global forum

Founded 2006

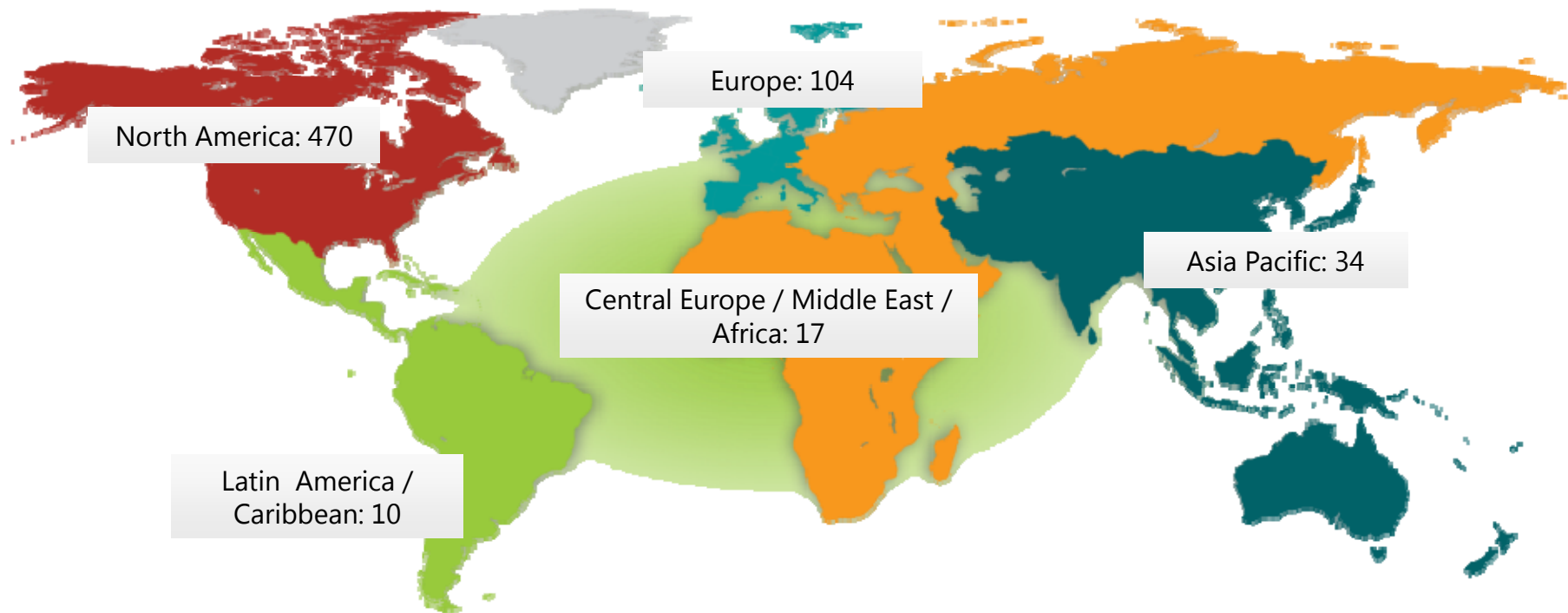
Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness



Global Growth

More than 600 organizations have joined



Continued and Sustained Growth

European Community Meetings

	2009	2010	2011
Total Attendees	171	272	457
PO Attendees	103	160	229
QSA/ASV/PTS Lab Attendees	68	121	140

New Guidance 2011



EMV



Telephone-based
Payment Card Data



Virtualization



Tokenization



Wireless



PA-DSS and Mobile



Agenda

About the Council

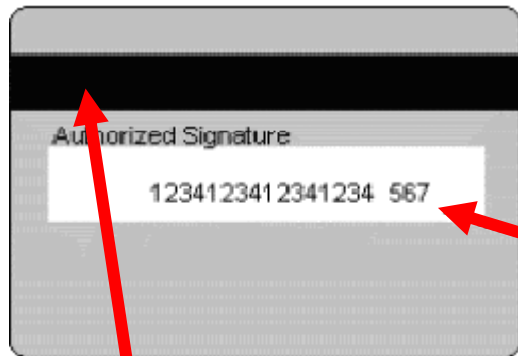
What is being protected?

The PCI Standards

Council Resources



What is the sensitive card information



Visa/MasterCard Security code

Track Data



Security code

PCI Update - Data Storage Clarification

	Component	Storage Permitted	Protection Required	Encryption Required**
Cardholder Data	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

* Data elements must be protected when stored in conjunction with PAN

** Compensating controls for encryption may be employed

Agenda

About the Council

What is being protected?

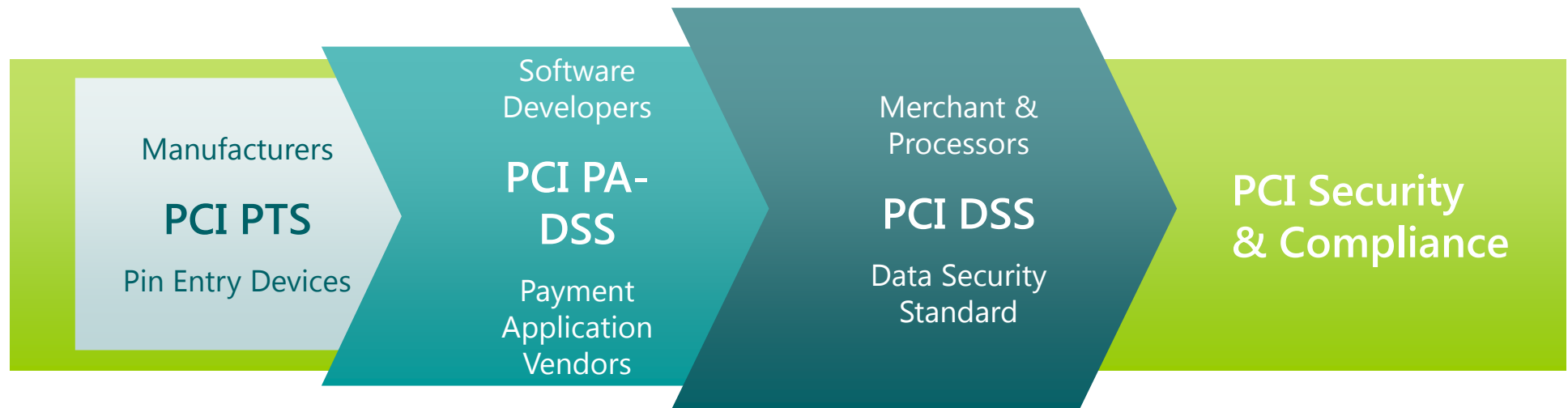
The PCI Standards

Council Resources



PCI Security Standards

Payment Card Industry Security Standards Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

The PCI Data Security Standard

Six Goals	Twelve Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors

Agenda

About the Council

What is being protected?

The PCI Standards

Council Resources



Website

The screenshot shows the PCI Security Standards Council website. At the top, the browser address bar displays "PCI Security Standards Council, LLC [US] https://www.pcisecuritystandards.org". The website header includes the PCI Security Standards Council logo, navigation links for Home, Contact, FAQs, and Change Your Language, and a search bar. A dark navigation bar contains links for For Merchants, PCI Standards & Documents, Approved Companies & Providers, Training, News & Events, About Us, and Get Involved.

The main content area features a large teal banner with the text "Welcome to the PCI Security Standards Council". Below this banner are four columns representing different user groups: Merchants (with a card terminal icon), Financial Institutions (with a skyscraper icon), Hardware / Software (with a computer monitor icon), and Services and Professionals (with a man in a suit icon). Each column includes a brief description and a "Learn More" link.

To the right of the main content, there is a section for "PCI DSS 2.0 and PA-DSS Version 2.0 Now Available!" with a link to download documents. Below that is an "EVENTS" section listing three upcoming events: NRF 100th Annual Convention & Expo (January 09, 2011), European Card Acquiring Forum (February 06, 2011), and 2011 Hospitality Law Conference (February 09, 2011).

At the bottom left, a "NEWS" section lists two recent announcements: "December 10, 2010 PCI Security Standards Council Announces PCI Forensic Investigator (PFI) Program" and "October 28, 2010 PCI Security Standards Council Releases PCI DSS 2.0".

At the bottom center, there is a "PCI ROCK Payment Card Security" graphic featuring a cowboy and three women. At the bottom right, there is a "Meet our Participating Organizations" section with a photo of a group of people.

Resources for Services and Professionals

PCI Security Standards Council, LLC [US] https://www.pcisecuritystandards.org

PCI Security Standards Council


Home · Contact · FAQs · Change Your Language

Search

For Merchants | **PCI Standards & Documents** | Approved Companies & Providers | Training | News & Events | About Us | Get Involved

Services & Professionals

Text size [-] [+] · Share · Print



Welcome to the PCI Security Standards Council's Services & Professionals area!

The PCI DSS 2.0 and PA-DSS Version 2.0 Now Available!

The latest version of the PCI DSS and PA-DSS is designed to provide greater clarity and flexibility to facilitate improved understanding of the requirements and eased implementation for merchants. Version 2.0 becomes effective on January 1, 2011.

- [Download PCI DSS v2.0](#)
- [Download PCI DSS Summary of Changes Version 1.2.1 to 2.0](#)

Press releases

December 10, 2010
[PCI Security Standards Council Announces PCI Forensic Investigator \(PFI\) Program](#)

October 28, 2010
[PCI Security Standards Council Releases PCI DSS 2.0 and PA-DSS 2.0](#)

October 21, 2010
[PCI Participating Organizations Finalize Feedback on Next Version of PCI Security Standards at Global Community Meetings](#)

DECEMBER 2010

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18

PCI Awareness Training – New for 2011!

A high level introduction to the Payment Card Industry and the PCI DSS

Who should attend?

Open to anyone who is interested in learning more about PCI, with a focus on those individuals working for organizations that must meet compliance with the PCI DSS or have a vested interest in the Payment Card Industry

What does it cover?

Key topics:

- What is PCI and what does it mean to a company that must meet compliance with the PCI DSS?
- Roles and responsibilities of the key actors in the compliance process
- How the credit card brands differ in their requirements for PCI reporting and validation
- Overview of the infrastructure used by organizations to accept payment cards and communicate with the verifications and payment facilities
- Real world examples of PCI challenges and successes

How can I sign up?

This course is offered both online and as a one day instructor-led session. Please visit the PCI SSC Awareness Training page on the Council website for an up-to-date schedule of courses and registration details:

https://www.pcisecuritystandards.org/training/non_certification_training.php

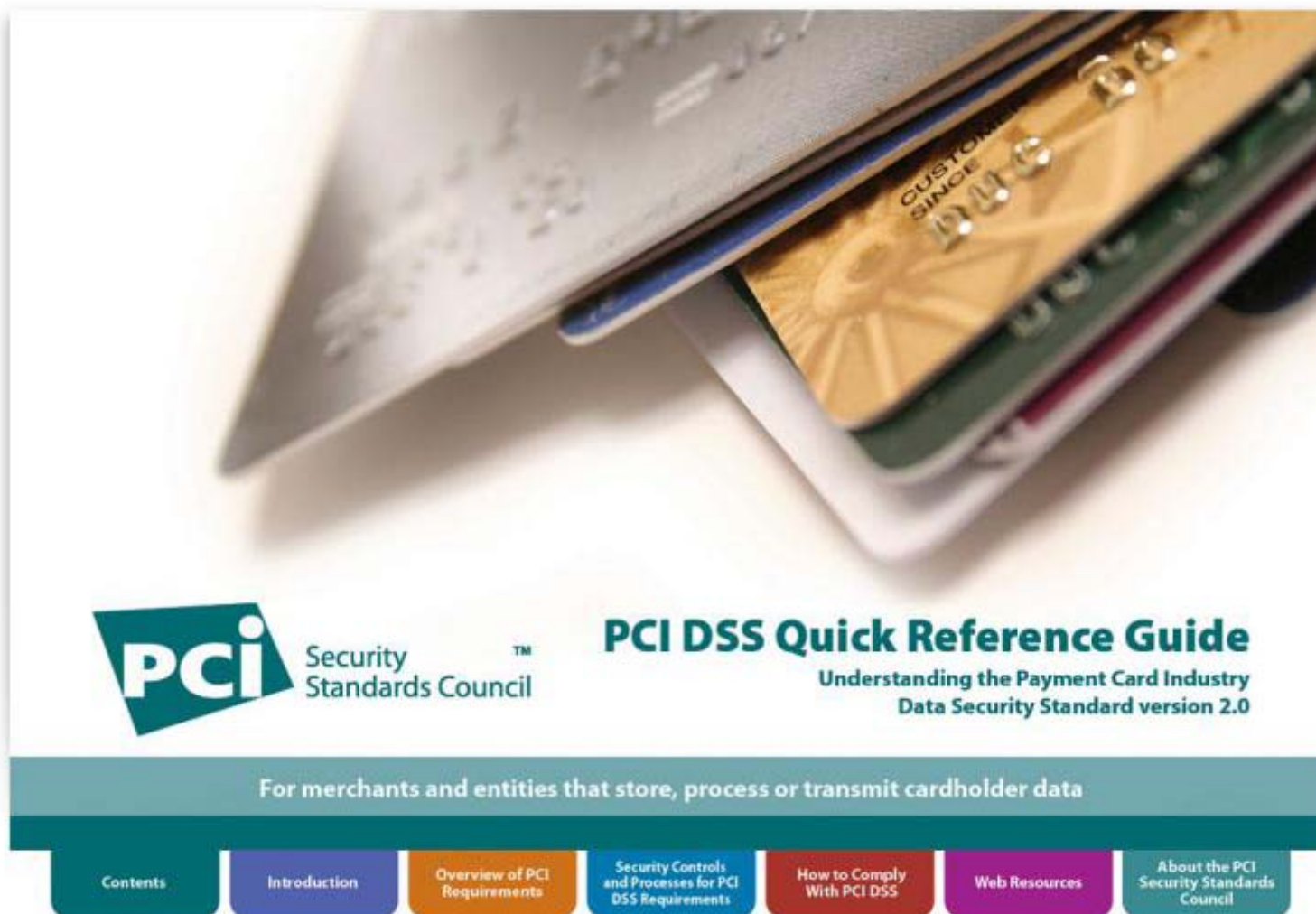
**Awareness Training
available online!**

Dates & Cost

Fees: \$995.00 per individual (plus VAT where applicable)

Online: (per company) 1-24 people \$495; 25- 99 people \$395; 100+ people \$295

PCI Quick Reference Guide



Council Resources

Security standards
and supporting
documents



Quick Reference
Guide



Searchable
Frequently Asked
Questions



List of approved
QSAs, ASVs, PA-
QSAs, PED Labs



Education and
outreach - e.g.,
fact sheets,
webinars



Participating
membership,
meetings,
collaboration



A global voice for
the industry



Questions?

Any Questions?



Please visit our website at www.pcisecuritystandards.org

Appendix

New Guidance 2011



Information Supplement: PCI DSS in EMV Environments

Key Recommendations:

- EMV and PCI DSS are both essential elements in the fight against payment card fraud and data exposure
- EMV mitigates the risk of counterfeit card fraud in face-to-face environments
- PCI DSS remains necessary in EMV environments to mitigate risk of fraud in non-EMV channels
- EMV + PCI DSS = powerful approach to reducing fraud and increasing security

New Program – P2PE Hardware/Hardware



Point-to-Point Encryption (P2PE)

Introduction:

- The Council delivered *Initial Framework on Point-to-Point Encryption* guidance in October 2010
- P2PE solutions may help merchants reduce scope of their CDE and their PCI DSS assessment
- The Council now has the first set of P2PE validation requirements for hardware-based encryption and decryption solutions
- Developed with the Encryption Task Force
- Supporting testing procedures, assessor training, and other resources coming Q4 2011 and early 2012

New Guidance 2011



Information Supplement: Telephone-based Payment Card Data

Key Recommendations:

- Identifies risks and considerations specific to telephone-based payment card data
- Provides a step-by-step flowchart to help determine PCI DSS controls for voice recordings
- Specific guidance addressing capture of SAD
- Identifies several applicable PCI DSS requirements with recommendations specific to call recording environments
- Provides sample questions that merchants can ask call center providers to determine how their solution supports PCI DSS compliance

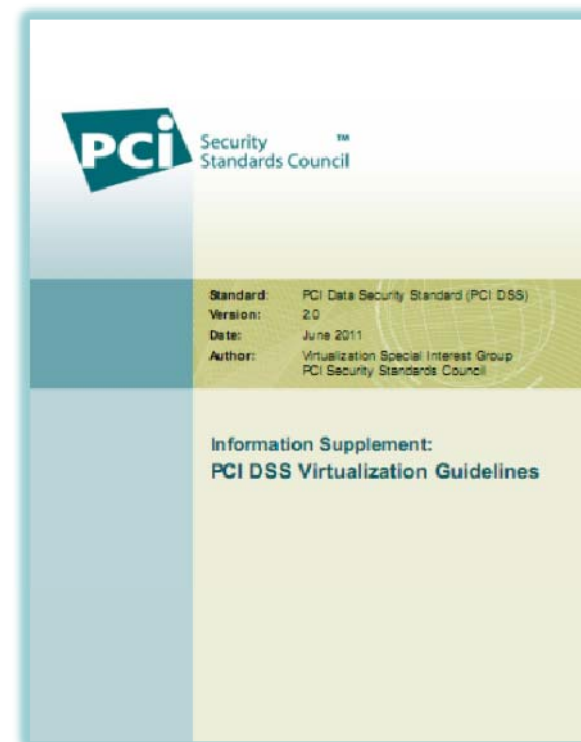
New Guidance 2011



Information Supplement: Virtualization

Key Recommendations:

- Perform thorough evaluation of the technology and the impact on PCI DSS
- Specific security considerations for virtual environments
- Recommends all virtualization components meet PCI DSS requirements
- Defense in depth approach across both physical and logical layers



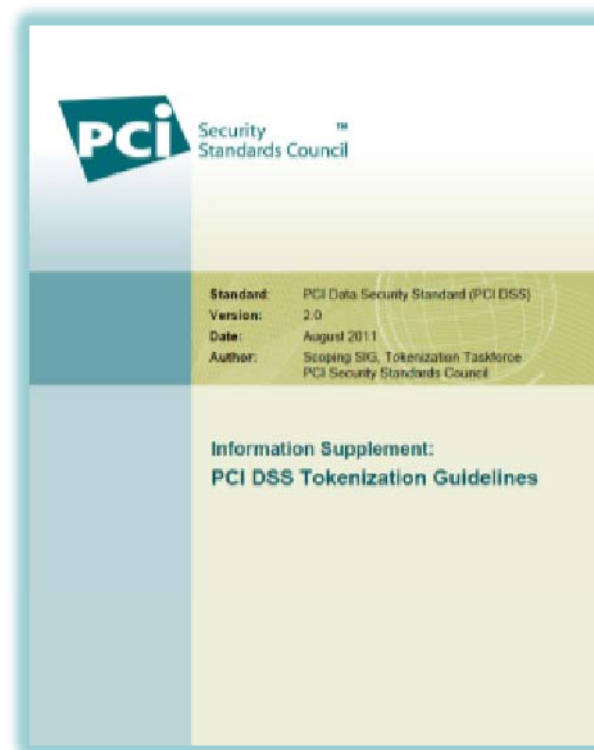
New Guidance 2011



Information Supplement: Tokenization

Key Recommendations:

- Tokenization does not eliminate the need for PCI DSS
- Primary goal is to replace sensitive PAN values with non-sensitive token values
- Tokenization may affect PCI DSS scope by limiting systems that store, process or transmit cardholder data
- Tokenization can contribute to a layered approach to cardholder data security





Information Supplement: Wireless

Overview:

- Updated guidance aligns with PCI DSS v2.0
- Incorporates Bluetooth technologies
- Recommendations for securing wireless technologies
 - Expanded guidance
 - Testing and detecting rogue wireless access points per PCI DSS 11.1

The image shows the cover of the 'Information Supplement: PCI DSS Wireless Guidelines'. At the top left is the PCI Security Standards Council logo. The cover is divided into four quadrants by a vertical blue line and a horizontal green line. The top-right quadrant contains the following text: **Standard:** PCI Data Security Standard (PCI DSS), **Version:** 2.0, **Date:** August, 2011, **Author:** Wireless Special Interest Group (SIG), PCI Security Standards Council. The bottom-right quadrant contains the title **Information Supplement: PCI DSS Wireless Guidelines**. The background of the cover features a faint globe graphic.

New Guidance 2011



PCI SSC Update June 2011 Mobile

Update & FAQ on applicability of PA-DSS to mobile payment acceptance applications

- Category 1 and 2 applications are eligible for PA-DSS
- Category 3 applications are pending development of further guidance and/or standards

Category 1
PTS Approved PED
Devices

Category 2
Purpose Built POS
Devices

Category 3
General Purpose
Smart Device