Request for Feedback PCI PIN v3 Instructions

Request for Feedback PIN v3

These security requirements have been updated. Significant updates include:

- Based upon industry feedback, the requirement that encrypted symmetric keys must be managed in structures called key blocks has been revised and broken into three separate phases, with different implementation dates.
- The usage of personal computers for key loading, where clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of a secure cryptographic device (SCD), is being phased out at future dates.
- The allowance for the injection of clear-text secret or private keying material into an SCD is being phased out at future dates. Only encrypted key injection shall be allowed.
- The test procedures have been enhanced to ensure more robust testing of existing requirements.

How to use the portal

- Go to the portal, https://programs.pcissc.org/default.aspx
- Log-in with your username and click “Forgot your password” to create a new password
- If you do not have a username, please let the Program Manager know by emailing pcipts@pcisecuritystandards.org and you be will sent you your username
- Accept the NDA
- When you enter feedback through the portal, you must fill in the section or requirement number and specific comments for that section (be as detailed as possible)
- Please remember to “Save draft comments” after each entry to ensure your work is saved
- Each company must consolidate feedback and can only submit once. Feedback is limited to 50 entries.
- Once you are done entering all of your feedback, select “submit feedback” at the bottom of the screen
- It will ask you if you are sure, select “Ok”. Once you submit your feedback you will receive a confirmation email

Summary

- Comment period opens 18 August 2017
- Please check the portal to ensure you have access
- Comments must be in by 11:59PM ET on 18 September 2017

- Please contact the Program Manager with an questions or concerns
  - pcipts@pcisecuritystandards.org

- https://programs.pcissc.org/default.aspx

Thank you in advance for your feedback!