Request for Comments Instructions: PCI PTS POI V6.2

Thank You in Advance!

First and foremost, the PCI Council would like to thank you for taking time to review this draft of *PCI PTS POI V6.2*.

Your thorough review of the areas associated with these changes is welcome and is fundamental to our revision process. The following slides will guide your review.

RFC Overview: PTS POI V6.2 RFC

- Efforts are underway to update the PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements documents. This consists of two documents:
  - PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements
  - PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements

- PCI SSC is targeting publication of the PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements during 2nd quarter 2023.

- The update includes the reformatting and renumbering of the requirements with the addition of the test procedures.

Timeline for PTS POI V6.1 RFC

- The RFC period will run from Thursday 1 September 2022 through Friday 30 September 2022.
- Be sure to submit all feedback to the Portal by 8:00pm Eastern Time on Friday 30 September 2022.

Note: *PCI SSC can only accept feedback that is received via the Portal during the RFC period. Late feedback and feedback submitted via any other channel will not be accepted.*

Your Feedback

To help get the most out of your feedback, please be sure to:

- Read this RFC guidance in its entirety before beginning your review.
- Read the *PIN Transaction Security (PTS) Point-of-Interaction (POI) Summary of Requirements Changes from Version 6.1 to 6.2* before reviewing the standard and refer to it during your review.
- Identify the document, page, section/requirement, and sub-requirement (if applicable) that your feedback refers to.
- Please be as detailed as possible with your comments and feedback.
- Please note if test procedures collectively provide sufficient testing to verify the associated security requirement. Was the test procedure a valid test for the security requirement (e.g., does not introduce additional requirements)? Could the test procedures be improved?
- Include suggested wording for addressing your comments in the Suggested Solution field. For example, suggest new content for clarifying a draft requirement or additional guidance to be included.
- Submit your feedback via the portal. **Feedback that is not provided via the portal will not be considered.**

Your Feedback (Cont.)

- As a reminder, you will be required to agree to a Non-Disclosure Agreement (NDA) to download the document.
- **Your feedback, your organization's name, and how PCI SSC actioned your feedback comments will be made available for review by RFC participants in the PCI SSC portal.**
  - Review the PCI SSC RFC Process Guide for more information
  - Please avoid including company sensitive information and remember to keep your comments professional and collaborative
- Each company is asked to consolidate their feedback and include a maximum of 50 feedback entries.

Accessing Documents and Submitting Feedback

- Go to the portal: https://programs.pcissc.org.
- Log-in with your username and password.
  - If you don't know your password, click "Forgot your password" to create a new password. If you do not have a username, please contact the Program Manager pcipts@pcisecuritystandards.org for assistance.
- Click on "*PCI PTS POI V6.2 RFC*"
- Accept the non-disclosure agreement (NDA).
- Click to download the documents.
- To enter feedback, select the Document, Section/Requirement, Sub-Requirement (if applicable), and Page Number.
- Enter your Comments and Suggested Solution for each feedback item.
- In the Comment field, explain the reason for your feedback.
- For example, describe why a requirement is unclear or how it is not applicable to a technology or implementation.
- In the Suggested Solution field, include your recommendation to address your comments.

Accessing Documents and Submitting Feedback (Cont.)

- For example, suggest new language to clarify an unclear requirement or for additional guidance.
- Be as detailed as possible with your comments and suggested solutions.
- The Comment and Suggested Solutions fields are required. If there is nothing to note for one of the fields, please input 'None'.
- There is no need to submit the same feedback item more than once. PCI SSC reviews every feedback item submitted.
- This is not the forum to submit questions. For questions regarding HSM, please send an email to pcipts@pcisecuritystandards.org
- Please remember to "Save draft comments" after each entry to ensure your work is saved.
- Once you have entered all your feedback, select **"Submit feedback"** at the bottom of the screen. You will be asked if you are sure. Once you select "Ok", you will not be able to add or edit your feedback. Upon submission of your feedback, a confirmation email will be sent.
- Alternatively, you can download the feedback spreadsheet, input your feedback, save, and then upload the file back to the Portal.

Who has access to the feedback?

- The primary contact(s) for your company can access the RFC documents via the Portal.
- The role of the primary contact is to coordinate your company's review of the RFC materials, collect and consolidate all comments and suggested solutions, and submit your company's feedback to PCI SSC via the Portal before the due date.
- If you are unsure who the primary contact is for your company, please contact participation@pcisecuritystandards.org for assistance.