

Read Me First

Instructions for EGTF Stakeholder Feedback:
Guidance for PCI DSS Requirements 6.4.3 and 11.6.1

Introduction

The PCI Security Standards Council (PCI SSC) would like to thank you for taking the time to review the draft guidance document for PCI DSS Requirements 6.4.3 and 11.6.1.

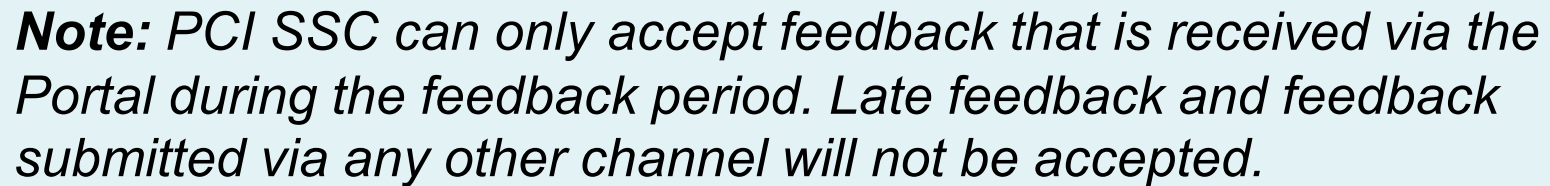
The following slides provide instructions and guidance that will assist you during your review.

Before You Begin

- **Please read these instructions and guidance in their entirety.**

Timeline for Stakeholder Feedback

- The review period will run from 5 February -11 February.
- Be sure to submit all feedback to the Portal no later than 11:59 pm Eastern Time on **11 February 2025**



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

Purpose of this Request

PCI SSC is requesting your feedback on the current draft guidance document for PCI DSS Requirements 6.4.3 and 11.6.1

Feedback received during this feedback period will be reviewed and considered for inclusion in this document.

Please note that feedback will only be considered if it relates to the contents of this guidance document.

Feedback Instructions

Accessing the Guidance Document

Note: Only your company's primary contact may log into the portal and download the guidance document. If you do not know who your company's primary contact is, please contact support@pcisecuritystandards.org for assistance.

- This feedback period is only available to the members of the E-commerce Guidance Task Force.
- Steps to access the document:
 1. Log-in to the PCI portal: <https://programs.pcissc.org>.
 2. If needed, reset your password via "Forgot your Password"
 3. Click on the draft *Guidance for PCI DSS Requirements 6.4.3 and 11.6.1*
 4. Accept the group Participation Agreement (the NDA).
 5. Download the document.

For access issues, contact support@pcisecuritystandards.org.

Submitting Feedback (1)

- To enter your feedback into the portal, select “Feedback Option 2”
 - Select “Save Draft Comments” after each entry and before you exit the portal.
 - You can finish entering feedback later; you do not need enter all feedback in the same session.
 - When all your feedback is complete, select “Submit Feedback” and “Ok” to confirm.
 - Once you select “Ok,” you will be unable to edit your feedback.
- Alternatively, select “Feedback Option 1” to download the feedback spreadsheet
 - After you input your feedback, upload the spreadsheet back to the Portal.
- A confirmation email will be sent after you submit your feedback.

Submitting Feedback (2)

- To enter feedback:
 - Select the Document Section, enter the page number, and select the feedback Category.
 - Enter your Comments and Suggested Solution for each feedback item.
 - In your comments, identify any section(s)/number(s) in the draft guidance document that your feedback refers to (if applicable).
 - If using the Portal to enter your feedback, remember to “Save draft comments” after each entry to ensure your work is saved.
- Consolidate your feedback since you can only provide 50 total feedback entries, one submitter per company.
- Contact support@pcisecuritystandards.org with any questions.

Maximizing the value of your feedback:

- In the Comment field, clearly explain the reason for your feedback.
- In the Suggested Solution field, provide a specific recommendation.
- Be as detailed as possible while keeping feedback concise.
- Avoid repeating the same feedback – each item is reviewed.
- It is not necessary to copy the same information into “Suggested Solution” and “Comment”

Please note that feedback will only be considered if it relates to the contents of this guidance document.

For Consideration While Providing Feedback

Editing Notes

- PCI SSC has edited the content provided by members of the E-commerce Guidance Task Force (EGTF) at the end of December.
- Some of the edits included:
 - Combining sections and eliminating redundant content.
 - Adding/revising tables to consolidate content.
 - Removing or editing content that indicated items were required by PCI DSS that are not required.
- Hopefully, the edits made the document more concise while keeping important content.

Refresh on EGTF Objectives

This information supplement provides guidance to help PCI SSC stakeholders understand and implement PCI DSS v4.x Requirements 6.4.3 and 11.6.1 effectively.

Guidance Objectives:

- Provide clear and actionable steps for meeting these requirements.
- Explain how third-party service providers (TPSPs) can support compliance.
- Focus on how to meet the requirements, rather than just their intent.

(From the E-Commerce Guidance Task Force Terms of Reference.)

Considerations for your Review

- Should any material be added from the “full collated version”, found in the Docs & Files section in Basecamp?
 - Link to the full collated version is on the next slide.
- Is anything inaccurate from a technical perspective?
- Does the document sufficiently meet the objectives* noted on slide 12?

Historical Document References in Basecamp

- Edited version from 13 January
 - Reviewed during 27 January EGTF meeting
- Full collated version of all EGTF input as of end of December 2024