# Request for Comments Instructions: RFC Draft PCI Secure Software v2.0 Standard

10 July to 11 August 2025



PCI Security Standards Council

# Thank You in Advance!

First and foremost, the PCI Council would like to thank you for taking time to review this RFC draft of the PCI Secure Software v2.0 Standard.

Your thorough review is welcome and is fundamental to our revision process. The following slides will guide your review.

→ **There is significant context in these ReadMe slides for this RFC. Read through each slide thoroughly.**

# RFC Overview

This is a major revision to the Secure Software Standard. There are considerable changes based on stakeholder feedback. Review the draft **in its entirety**.

The following slides will highlight significant changes along with questions to consider during your review.

# Two Documents

There are now two documents of note for this RFC:

Draft PCI Secure Software Standard, v2.0 (update from v1.2.1)
Draft PCI Secure Software Standard – Sensitive Assets – (*for use w/ v2.0*)  **NEW DOCUMENT**

# Sensitive Assets Document

~ NEW ~

A new external companion document called '*Sensitive Assets*' is being provided as part of this RFC.

This document is intended to be published with the Secure Software Standard, and it is a required companion document to the Standard. It is also used to set context for numerous security requirements.

This document is part of this RFC – provide constructive comments as applicable.

→ **For RFC feedback regarding this document, choose this specific document as the source 'document: "*Sensitive Assets Document*".**

# Sensitive Assets Document

**~ NEW ~**

This document has tables of examples for Sensitive Data, Sensitive Resources, and Sensitive Functionality. Your feedback and suggestions as encouraged.

→ **Provide constructive recommendations for example categories to be considered for the included Sensitive {Data, Functionality, Resources} tables, including descriptions and examples as relevant.**

→ **For RFC feedback regarding this document, choose this specific document as the source 'document: "*Sensitive Assets Document*".**

# Major Themes

**~ NEW & CHANGE~**

The following is a high-level outline of major objectives for this revision effort:

**- Removed the context of 'payment software'.**
**- Redesigned the nucleic context of Sensitive Assets**

} Fundamental Change

**- Removed redundancies**
  - within the Standard itself, especially between the Modules and Core
  - between SecSW and SSLC

**- Removed all language from Test Reqts that essentially constitute Security Reqts.**

**- Improved the objective degree of the Security Reqts.**

**- Restructured the organization and flow of the Standard, especially the Core section.**

**- Significant updates based on stakeholder feedback**

**- Increased the associativity between PAN/SAD in SecSW w/ PCI DSS.**

**- Added a new module for SDKs**

# Sampling

The context of sampling has been revised in the Introductory text in the draft standard.

Sampling does not apply to the software under assessment as there is only one unique instance of the software.

In addition, the context of populations of evidence (e.g., logs, etc.) that could be sampled should be rendered moot as the security reqts and associated test reqts requiring evidence of process have been removed.

# Question for the RFC: Draft Reqt 1A-1

**~ REQUEST for FEEDBACK ~**

As inclined, provide constructive feedback on the use of the term ‘BOM’ vs. the ***potential*** use of the term ‘SBOM’ in draft requirement 1A-1.

**Denote RFC feedback in association to reqt 1A-1.**

~ CHANGE ~

# Glossary / Terminology

The external SSF Glossary will be superseded by including applicable terms within the Secure Software Standard (Appendix A). This makes it easier to reference these terms from within the respective Standard.

In addition, defined terms in Appendix A that appear in requirement language will be denoted as follows for easy identification. E.g.,

**2A-1** The *sensitive data* of the software is identified and documented.

# Program Proposal for SW Changes

**~ REQUEST for FEEDBACK ~**

[Proposal on next slide]

- Introduce ’Wildcards’ for everyone
- Increase benefits to be a Secure SLC Qualified Vendor (Tier 1 Delta)
- Remove default stipulation for a Full Assessment for High Impact Changes (Tier 2 Delta)
- Delta Changes involve determining the ‘delta’ impact of the change to the previously established compliance of the software to the Secure Software requirements.
- Significant relation to the new draft definitions for Sensitive {Assets, Data, Resources, Functionality}

**Notes**: Low Impact → Tier 1 Delta
High Impact → Tier 2 Delta

→ **Denote RFC feedback in association to: ‘Program’.**

## Software Changes

| Impact | Change Type | Description | SSLC Qualified Vendors | Non-SSLC Qualified Vendors |
|---|---|---|---|---|
| **Non-security Impacting Changes** | **Wildcards** | Exclusively allowed for non-security-impacting changes made to the software product that have no impact on the security aspects of the software product and are not within the scope of any PCI Secure Software Standard requirements.<br>The use of wildcards is optional.<br>Wildcards cannot be used to account for Delta Changes. | **Allowable for Use** | **Allowable for Use** |
| | | | | |
| **Security-Impacting [Delta] Changes** | **Tier 1 Delta** | Any change to the software product that meets <u>any</u> of the following:<br>- Any non-security impacting change to the software where the version number of the software must change AND the software vendor is not using previously established wildcards as per the PCI Secure Software Program.<br>- Any change that does not involve or otherwise potentially impact sensitive assets, which includes sensitive data, sensitive resources, and/or sensitive functionality.<br>- Any security-impacting bug fixes/patches, even if they involve sensitive assets, which includes sensitive data, sensitive resources, and/or sensitive functionality. | **Not required to use Assessor** | **Required to use an Assessor** |
| | **Tier 2 Delta** | A change to the software product that meets **<u>any</u>** of the following:<br>- The introduction of a new sensitive {data, functionality, resource} type into the software product.<br>- Any change that results in the need to assess the software product to PCI Secure Software Standard requirements that were <u>NOT</u> previously assessed. This includes any individual requirements (e.g., a requirement that was deemed Not Applicable for a previous assessment) and/or entire ancillary modules of requirements.<br>- Any change that involves or otherwise potentially impacts sensitive assets, which includes sensitive data, sensitive resources, and/or sensitive functionality.<br>- Any change that involves requirements in an ancillary (non-Core) module that requires the previously established and noted support of that module to be revoked. | **Required to use an Assessor** | |

# Payment Software Type



**~ REQUEST for FEEDBACK ~**

It is the intent to remove for v2.x+ the listing element for ‘Payment Software Type’, as detailed in the PCI Secure Software Program Guide pg. 39,40.

→ **Denote RFC feedback in association to: ‘Program’.**

# ROV Reporting Instructions



**~ REQUEST for FEEDBACK ~**

We are exploring the idea of including the ROV reporting instructions within the Secure SW Standard itself, which will then be copied into the ROV with the Security and Test requirements as per usual.

This is only being considered for Secure Software, or SSF, at this time.

An illustrative mockup simply exemplifying the concept is on the next two slides.

# ROV Reporting Instructions



**~ REQUEST for FEEDBACK ~**

| Security Requirements | Test Requirements |
|---|---|
| **3-2** *Sensitive data* is only retained in non-persistent memory for the duration necessary, after which time it is securely deleted, if possible, else it is rendered unrecoverable. | **3-2.a Perform** static analysis to **verify** the sensitive data is securely deleted once it is no longer necessary to retain. If this is not possible due to a legitimate and verified technical constraint, then **verify** the sensitive data is rendered unrecoverable.<br>**Report** the static analysis performed, including if there are any legitimate technical constraints, which must include the required details as denoted in the *Technical Constraints* section in this standard.<br>**3-2.b Perform** dynamic analysis to **verify** the analysis and findings in 3-2.a. Testing should include, **but is not limited to**:<br>- Attempting to violate, bypass, or otherwise circumvent the methods employed to securely delete or render the sensitive data unrecoverable.<br>- Where a technical constraint is stated, verify the technical constraint.<br>- Attempting to recover sensitive data after being securely deleted or otherwise rendered unrecoverable.<br>**Report** the dynamic analysis performed including verification of any legitimate technical constraints. Include details on the type of testing or test cases utilized, in conjunction with the information from 3-2.a, to verify the requirement is satisfied. |

**Notes:**

- In the future, if this is adopted, this would mean the reporting instructions will be part of the RFC of the Standard.

→ **Denote RFC feedback in association to: 'Program'.**

# ROV Reporting Instructions



**~ REQUEST for FEEDBACK ~**

**Security Objective 3: Sensitive Asset Storage and Retention**

Sensitive assets are stored in a secure manner commensurate with their data type and use and retained for only as long as necessary.

| Notes: | | | | |
|---|---|---|---|---|
| **Security and Test Requirements** | **Reporting Instructions** | **Assessment Findings (*select one*)** | | |
| | | **In Place** | **Not Applicable** | **Not in Place** |
| **3-2** *Sensitive data* is only retained in non-persistent memory for the duration necessary, after which time it is securely deleted, if possible, else it is rendered unrecoverable. | | ☐ | ☐ | ☐ |
| **3-2.a Perform** static analysis to **verify** the sensitive data is securely deleted once it is no longer necessary to retain. If this is not possible due to a legitimate and verified technical constraint, then **verify** the sensitive data is rendered unrecoverable. | **Report** the static analysis performed, including if there are any legitimate technical constraints, which must include the required details as denoted in the Technical Constraints section in this standard. | *<Assessor response here>* | | |
| **3-2.b Perform** dynamic analysis to **verify** the analysis and findings in 3-2.a. Testing should include, **but is not limited to**:<br>- Attempting to violate, bypass, or otherwise circumvent the methods employed to securely delete or render the sensitive data unrecoverable.<br>- Where a technical constraint is stated, verify the technical constraint.<br>- Attempting to recover sensitive data after being securely deleted or otherwise rendered unrecoverable. | **Report** the dynamic analysis performed including verification of any legitimate technical constraints. Include details on the type of testing or test cases utilized, in conjunction with the information from 3-2.a, to verify the requirement is satisfied. | *<Assessor response here>* | | |

**Notes:**

- In the future, if this is adopted, this would mean the reporting instructions will be part of the RFC of the Standard.

→ **Denote RFC feedback in association to: 'Program'.**

# RFC Timeline:

- The RFC period will run from 10 July 2025 through 11 August 2025.
- Be sure to submit **all** feedback to the Portal **on or before:** 8:00pm Eastern Time on 11 August 2025.

***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****.*

# RFC Feedback Guidelines

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

- Identify the document, page, section/requirement, and sub-requirement (if applicable) that your feedback refers to. **Ensure the feedback item is obvious in what it refers to**.
- Use the '*Comment'* field to succinctly capture your feedback.
- Use the '*Suggested Solution*' field to recommend a solution based on the Comment. **Do NOT copy/paste the Comment into the Suggested Solution or otherwise duplicate the entries between the two fields.**
- When providing feedback that relates to more than one requirement, simply create one entry and denote the requirements your comment applies to. **Do NOT create multiple entries all with the same comments/suggested solutions.**
- **Ensure your feedback is constructive.**
- **Note there are options to select other documents aside from the Standard – use those as applicable.**
- **Denote Tech Writer-esque comments with the 'TW' category.**

# Important Items of Note

- Submit your feedback **via the portal.** **Feedback that is not provided via the portal will not be considered.**
- **Submit your feedback on or before the due date.**
- Agreement to a Non-Disclosure Agreement (NDA) to download the document **is required**.
- **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 at a **maximum of 75 feedback entries**.

# 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.

# 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 software@pcisecuritystandards.org for assistance.
- Click on "*PCI Secure Software v2.0 RFC Draft Standard*"
- Accept the non-disclosure agreement (NDA).
- Click to download the document.
- Toenter feedback, select the Document, Section/Requirement, Sub-Requirement (if applicable), and Page Number.
- Enter your Comments and Suggested Solution for each feedback item.
- 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.