7:41 AM PDT 2023-04-26

**Call to Order:** 0805

**Meeting Lead:** Brandon HARVEY (Josh away)

**Attendees:** 18

**Member Count:** 70

**Next Meeting:** Wednesday May 3rd, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Modified the “High Level Process Overview” section in the Guidance document as follows:
  + - *“Review this guidance document and associated instructions*
    - *Map Assumptions, Security Objections for the Operational Environment, and Organizational Security Policies to applicable authorization scheme(s) as a reference implementation (FedRamp, C5, etc)*
    - *Summarize this mapping in generic language for wider Cloud Authorization adoption i.e. consideration in other authorization schemes*
    - *Determine the extent to which SFRs and SARs in the PP can rely on the OE to be satisfied so that the extent to which the TSF may need to rely on cloud services can be determined.*
    - *Identify SFR challenges in a cloud operational environment*
    - *For example certain requirements collecting test evidence may be complicated by the cloud operational environment and may not be directly accessible due to cloud isolation.*
    - *Many TOEs that will operate in a cloud environment will utilize object storage as provided by the CSP. These objects will often be encrypted either by the TOE itself or by the CSP. For instances in which the CSP is providing encryption of the storage object, it is expected that the TOE vendor or evaluator will not be able to perform assurance activity tests with regards to Key Destruction. PP authors will be expected to make modifications to related SFRs to allow for CSP Key Destruction or Zeroization as additional selections.*
    - *Such modifications may be made by iterating the underlying SFR in a base PP into a "Cloud" PP module which provides the cloud-specific selections and assurance activities.*
    - *Identify SAR challenges with either new/updated SAR’s and/or determine if applicable*
    - *For example AVA may have different considerations for a cloud operating environment depending on the TOE or PP. See Vulnerability Assessment Methodology for more information.*
    - *Edit cPP/PP and add new optional or selection based SFRs/SARs for cloud evaluations*
    - *Update cPPs supporting documents with new cloud requirements and applicable assurance activities.”*
  + Discussion around Key destruction requirements and how they would pertain to cloud environments. For example, in PPs if there is a key generation SFR, there is usually an associated SFR for key destruction when keys are no longer needed.
* Modified the “Vulnerability Assessment Methodology” section in the Guidance document as follows:
  + - *“In general, the AVA methodology shall be sufficient for most TOE types. However, certain edge cases may present themselves.*

*As we have introduced a trusted platform concept, underlying vulnerabilities in the cloud operating environment can be treated as they are in traditional OE analysis.*

*However, when applicable vulnerabilities are discovered or suspected for TOEs operating in a cloud environment the means in which evaluators are expected to shift negative test coverage must utilize cloud attack vectors. I.e. service portal, management plane, etc. “*

* + Discussion on how vulnerability assessment might be different on different cloud deployments vs on prem.
* “OWASP Cloud Top 10” Sections removed since we no longer are including it in this guidance document.

**Questions/Follow-ups:**

**~**

***End of Meeting – Adjourned 0855 PDT***