7:52 AM PDT 2023-04-19

**Call to Order:** 0800

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

**Attendees:** 19

**Member Count:** 70

**Next Meeting:** Wednesday April 26th, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Resumed discussion on ‘Guidance for Establishing Test Environments on Cloud Infrastructure’
  + Conceptually there isn’t much more to discuss on this topic since how a lab would stand up this environment is outside the scope of this working group effort.
  + However additional language may be needed in the guidance document to cover high level recommendations.
* Reviewed Issue #47 – “Steps for Adding “CC in the Cloud” to a PP”
  + “ High Level Process Overview section currently exists in the guidance document but was amended 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.*
    - *ID SFR "challenges" in a cloud operational environment*
    - *Address challenges with new/updated SFRs and/or determine if applicable*
    - *ID SAR "challenges with either new/updated SAR’s and/or determine if applicable*
    - *Edit cPP/PP and add new optional or selection based SFRs/SARs for cloud evaluations*
    - *Update cPPs supporting documents with new cloud requirements”*
* Removed section “OWASP Top 10” from guidance doc since we are not targeting those specifically anymore.
* Reviewed Issue #36 – Equivalence
  + Incorporated language drafted in previous meeting into the guidance document
  + Guidance document section “Cloud Topology” was created and amended as follows:
    - *“Placeholder for diagram discussed at workshop”*
  + Section “Cloud Equivalence Considerations” added to guidance doc and amended as follows:
    - *“We believe that, in general, products must be tested individually on each cloud platform. For example on Azure, On AWS, etc.*

*The Cloud Service Offering (to include cloud region or datacenter) must be detailed in the TOE evaluated configuration details. CSOs can not inherently be assumed to be equivalent. For instance, CSPs may have separate environments between government or commercial customers. However, if existing cloud authorizations exist for multiple regions or datacenters this may inform equivalency claims. Especially if the Trusted Platform meets the assumptions and objectives of the PP and is consistent across multiple cloud regions.”*

* Issue #32 closed as it is a duplicate of issue #36
* Reviewed Issue #83 - NIAP Policy 5 – CAVP OE Listing
  + Discussion on what would appear on CAVP certificates
  + Overall consensus that it’s reasonable for a CSP to provide the underlying hardware/CPU information to a customer to address this in a CAVP cert.
  + Jade S raised a potential issue that this may be too scheme specific and not generic enough for the overall global audience, and more generic language should be used here
  + Section “CPU Equivalency” in guidance document was amended as follows:
    - *“Applicable guidance shall be followed when labeling Operational Environments. (Reference to CAVP FAQ as an example). TOE’s that are being evaluated in a cloud context are expected to be able to conclusively demonstrate knowledge of the underlying TOE Platform for these specifics. If SFR enforcing functionality is agnostic to the TOE platform, such equivalency claims may be made.*

*E.g. CPU model / OS / Hypervisor / Guest OS / Container shall be defined where appropriate.*

*At this time, if a TOE is reliant on the OE for cryptographic operations, there is no need to leverage the related collateral that explicitly states operation for a given Cloud Provider. This equivalence rationale should also be considered when a TOE vendor is reliant upon a CSP for algorithm certification and many TOE platforms are claimed.”*

* + Issue #83 now closed.
* Justin F provided an updated that MDM Subgroup still working to get FedRamp materials to review, and more progress to be made in the next few weeks.

**Questions/Follow-ups:**

**~**

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