7:29 AM PST 2023-01-11

**Call to Order:** 0730

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 13

**Member Count:** 68

**Next Meeting:** Wednesday January 18th, 2023

**Next Trusted Provider Sub-Group Meeting:** Wednesday January 25th, 2023

**Highlights:**

* Draft Agenda for In-Person event presented by Josh
  + – Any mapping of SFRs to other requirements (eg 800-53) should be completed prior to in person, not to be done at in-person
  + Call for comments on all documents prior to the offsite meeting. It is requested that all attendees review the following:
    - Read and be familiar with ESR;
    - Read and provide comments on Guidance document;
    - Read trusted provider/platform proposal;
  + All comments and issues should be logged in GitHub.

**Old Business:**

~

**New Business:**

* Review of existing materials and discussed merging of draft documents
  + All CCitC members should review existing draft documents and provide any comments prior to the offsite meeting.
* Discussion on how Trusted Platform fits into the broader Trusted Provider and overall CCitC project.
* Discussion on the key factors that a Trusted Platform/Provider should offer
  + Consistent platform / operational environment
  + Physical security
  + Personnel security
  + Auditing
  + Data sovereignty / isolation
  + Tenant isolation – Virtualization PP provides SFRs for VM security features such as libvirt/qemu/etc, however the GPOS PP does not have SFRs for validating container sandboxing implementations such as secompfilter, etc.
  + Network segmentation
* Discussion on the demarcation point between a ”product” and a “service”.
* Justin F raised an open question currently with NIAP on NIAP policy 5 regarding the “exact match” terminology for CAVP requirements, but how leveraging a certified OS versus acquiring CAVP certs and whether there are any additional benefits to claiming/citing the OS Certificates.
* Discussion on how platforms can become trusted platforms and what the potential criteria for this definition could be including:
  + *“A recent common criteria certificate for each critical component (to be defined) in the platform being utilized by the TOE is preferred. Equivalency should be considered.”*
  + *“The Trusted Platform should be available for use on a given Cloud Service Provider’s offering. Specifically, it should be offered on the service being tested.”*
  + *“The cloud service being utilized must undergo continuous monitoring, inherit the assurance maintenance from the existing authorizations (FedRAMP for US, various European schemes eventually to be replaced by EUCSA scheme, etc.) by an authorized 3PAO (for US) and/or testing bodies”*
  + *“The actual evaluation must be conducted on the same service being claimed as trusted.”*
  + *“NVLAP requires your test environments to be isolated. A primary feature of cloud deployments is multi-tenancy which provides isolation for different customers. To discuss is how to document this requirement and ensure it is viable for evaluations. Clearly a trusted provider must be able to provide this isolation.”*

**Questions/Follow-ups:**

* **Jade S to investigate existing requirement mappings available from NIAP.**
* **Next CCitC meeting to include discussions on CAVP, Equivalence, and Assurance Continuity topics in order for members to raise questions and flag issues for NIAP to provide additional context and information on prior to the offsite meeting.**

***End of Meeting – Adjourned 0900 PST***