7:47 AM PDT 2023-04-05

**Call to Order:** 0804

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 22

**Member Count:** 70

**Next Meeting:** Wednesday April 12th, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Follow-up with action item for Anne G To ask FedRAMP auditors if bare metal testing is done.
  + Anne advised that pen testing is conducted as part of the overall process, however whether it is done on bare metal is unclear. Jade S is the FedRAMP liaison and will follow up with FedRAMP.
  + This issue to remain open until we have comment from FedRAMP
* Continued working on Guidance Document
  + Section “Guidance for Establishing Test Environments on Cloud Infrastructure”
    - Discussion on the use of evaluated configuration guidance with respect to the test environment. While an evaluator may not be able to perform some of the steps in the CC guidance document due to CSP restrictions, there must be a means in which to confirm that those configurations have been made and the environment/TOE is indeed in the described evaluated configuration.
    - A CC lab should be prepared to create and offer cloud testing infrastructure to TOE developers.
* Jade S advised that NIAP has put together a small group to continue the work of Justin F on the MDM PP analysis.
* Discussion on the gaps between requirements for FedRAMP authorizations vs CC.
  + FedRAMP testing does not go down to the same level/granularity as CC assurance activities. This can change depending on the particular SFRs and Assurance activities for a given PP.
  + A CC cert would aid FedRAMP more than a FedRAMP authorization would aid CC
    - However a FedRAMP authorization would aid a CC evaluation in the context of potentially defining a “Trusted Platform”.
* Looked at Issue #36 – Equivalence
  + “*Testing on one CSP, can this be applied to other CSP’s? What are the barriers? How to achieve? What are the steps? What arguments would be acceptable.”*
  + Discussion on this topic
    - Different CSPs will implement different features and security functions in various ways, therefore there may not be exact equivalence.
    - Anne G made the point that AWS east/west vs Gov Cloud are different environments and may not be equivalent in their security implementations. So testing would have to be done on both environments.
    - 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.
  + Discussion on a point that James D made regarding the customer base for potential CC in the Cloud evaluations.
    - Some customers may require or desire a higher security baseline depending on their use cases. For example, some vendors only pursue the CC certification whereas other will pursue CC certification plus a CSfC listing, where additional requirements may be levied.

**Questions/Follow-ups:**

* Jade S to follow up with FedRAMP regarding details on bare metal testing

***End of Meeting – Adjourned 0900 PDT***