7:48 AM PDT 2023-03-22

**Call to Order:** 0803

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 23

**Member Count:** 70

**Next Meeting:** Wednesday March 29th, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Continued where we left off last meeting with addressing issues in GitHub:
  + Issue #33 – Define Trusted Provider
    - Josh indicated that “Trusted Provider” is referenced in the ESR so a definition should be added for clarity.
    - Matt Downey (per his comment on GitHub) referenced a definition that was discussed during the September 7th, 2022 meeting: “*A trusted provider provides a trusted platform*”.
    - Discussion on this definition and how this term might be relevant to evaluations
      * Andy N raised the point that we don’t exactly know what the requirements are for a “Trusted Provider” yet, and we don’t know if FedRAMP will cover it. Andy N Suggested we set this issue aside for now, until we have more information on what requirements may be needed for a trusted provider vs platform.
      * Agreement among members to put this issue on hold for now and return to it at a later date.
  + Issue #35 – Bare Metal vs Multi Tenant
    - *Is bare metal required for cloud testing?*
    - Josh suggested that the schemes may need to reconsider whether bare metal is really needed for testing.
    - Randy suggested that bare metal is more or less a private instantiation of the cloud.
    - Anne suggested we ask FedRAMP if any testing is done on bare metal
    - General discussion on Private vs Public cloud implementations and how testing might be done on each and what PP’s typically require:
      * Generally, testing must be done on an isolated network
      * Justin Fisher reiterated that preparative procedures (AGD) must be followed with single vs multi-tenant environments being clearly documented (with any differences). For vulnerability analysis, if you have a multi-tenant environment, it must be clear how isolation is achieved. Justin mentioned that on previous versions of the NDcPP, if you’re deploying a virtual TOE, it must be the only VM running on the hypervisor in order to prevent VM bleedover, etc.
      * Test activities should describe what to consider and how the operational environment can ensure security.
      * Justin Fisher suggested that evaluation activities within NDcPP do not really change much for either physical or virtual TOE deployments. Test activities in a given PP should still be able to be completed in a cloud environment and those that cannot should be identified and can be incorporated as an addendum to the PP’s. Would eval testing activities be different in bare metal vs multi tenant? Likely not.
      * Some test evidence required may not be possible in the cloud, such as key destruction, or PCAPs.
      * At the IaaS level, GPCP, DSC, and possibly FDE likely must be bare metal. At the PaaS level GPOS, VMM, and DBMS multi-tenant is fine. At the SaaS level, either is fine but guidance is key and will likely require changes compared to on-prem guidance.
    - Josh reminded the group that we are not rewriting PP’s, we are giving guidance to the PP authors and if they have issues, they can come back to us and we will updated the guidance accordingly.
    - This issue to remain open for further discussion.
  + Issue # 74 – Lab/Evaluator Instructions
    - Discussion on what labs/certifiers need to consider to expand their scope to CCitC
    - Provide guidance to labs (and schemes) on how labs can maintain independence of the testing environment from the Cloud provider.

**Questions/Follow-ups:**

**~**

***End of Meeting – Adjourned 0856 PDT***