7:31 AM PST 2023-01-25

**Call to Order:** 0732

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 19

**Member Count:** 68

**Next Meeting:** Wednesday February 1st, 2023

**Next Trusted Provider Sub-Group Meeting:** Wednesday February 8th, 2023 **(@ In-person meeting)**

**Highlights:**

* Josh posted instructions on how to log an issue in GitHub. Instructions located in the Discussions section of OnlyOffice in the “Details about the Workshop” post.
* Josh has recruited Elaine Newton as a facilitator for the Offsite meeting, to help keep things organized and discussions moving along.

**Old Business:**

* Revisited topic of Trusted Provider
  + Matt Downey recalled that last year we agreed to focus on Trusted Platform before looking at Trusted Provider.
  + Josh Logged a GitHub issue to discuss and define the criteria and metrics required for a “Trusted Provider” as a topic for the Offsite meeting.

**New Business:**

* Discussion on CAVP, Equivalence, and Assurance Continuity.
  + Josh Identified that CAVP is largely consumed by USA & CAD. Matt Downy confirmed that many other countries still acquire CAVP certs in order to be listed on the NIAP PCL.
  + Andy Nissen raised the question of what other schemes (BSI/German for example) do to handle crypto and recognize equivalency.
  + Josh started a discussion on what would be missing for cloud evaluations when attempting to acquire CAVP vs an on prem hardware appliance
    - Justin Fisher suggested finding how variable the cloud instance is and whether there is any guarantee of hardware and operating system the TOE would be run on and to what extent the vendor would have control over the hardware in the operating environment.
      * In an on-prem environment, the admin/TOE vendor can deliberately choose to deploy on whatever hardware, and if it deviates from the evaluated config then there is risk acceptance, however in the cloud that decision could be made (knowingly or unknowingly) for the customer.
    - Customers need to identify what hardware platforms are available in the cloud environment and what crypto would be implemented by (platform, vs the TOE itself), and whether it’s an off the shelf solution (such as openssl) or a custom module developed by the TOE vendor.
    - Today’s requirements for CAVP include CPU, Chipset, O/S, Hypervisor or container
      * This information should be obtained by the customer from the CSP.
      * This raises the issue of bare metal vs multi-tenant cloud environments.
    - Discussion on some language used in the Draft CMVP Management Manual (v1.2) regarding remote testing of software and hybrid software modules, section 7.4:
      * *“The network access to a remote test operating environment shall be authorized and controlled by the vendor.The cryptographic module under test SHALL be confirmed to be running on an OE that is well-defined and has a specific OS version, hardware platform and version, and processor (including microprocessor version), as shown on the module’s certificate and security policy and where this can be confirmed during the test session. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud) may be used if these rules are met and the operating environment provides the same or additional level of security as the lab would provide for internal testing.   
        The tester shall have control (oversight) of the testing environment. The tester’s network shall be connected to the vendor’s network via a secure connection (e.g., VPN or SSH) as permitted within a signed agreement by the lab and vendor. The tester’s tools must satisfy the lab’s network requirements before connecting to the vendor’s network to test the module.”*

**Questions/Follow-ups:**

* Equivalency topic to be discussed at in-person meeting in Annapolis Junction
  + Testing on one CSP
    - Can this be applied to other CSP’s? what are the barriers? What arguments should be acceptable and how can this be achieved.

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