7:57 AM PDT 2023-05-03

**Call to Order:** 0801

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 17

**Member Count:** 70

**Next Meeting:** Wednesday May 10th, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Josh suggested creating an editorial subgroup when a more complete version of the document has been completed.
  + Andy Nissen agreed that having a smaller subgroup would be more efficient than having the whole group do editorial reviews.
  + Larger group to possibly work on the more complex issues and the smaller groups to work on more scoped and focused issues.
* Today will be comprised of working on some of the missing pieces of the first few pages of the Guidance Doc and next week break out into smaller editorial groups to complete some of the larger chunks of the rest of the documents.
  + Andy N advised that when various groups break off it can be hard to track whether all the pieces being generated align with each other in the context of the whole document, there must be consistency and flow.
* Created definition for ‘Hosting Environment’
  + Issue #88 called for the exclusion of “execution environment” term in favor of “hosting environment” Definition of “Hosting Environment” confirmed as follows:
    - *“Hosting Environment consists of everything that is outside the TOE boundary and is equivalent to the CC term "Operational Environment."*
* Considered the definition for “Trusted Cloud Service Provider (TCSP)”
  + This definition to be determined – will come back to at later date, since it may have an impact on ESR.
  + Jade S advised that Matt D suggested that the guidance doc would supersede what is in the ESR so therefore the ESR would not have to be changed, and in theory, the Trusted Provider term could be removed all together and not addressed.
  + Brief discussion on what the ramifications of pulling that definition would be. This issue will be revisited in the future as it could have a greater impact on the rest of the document and expectations from the ESR.
* Modified the definition for “Cloud Service Provider (CSP)” as follows:
  + *”A cloud service provider, or CSP, is a company that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals.”*
* Discussion on a potential definition for “Cloud Authorization Scheme”
  + This definition was created as an issue in GitHub (#93) for further research and investigation to gather information.
  + Brandon H created the following rough definition:
    - *“A regulatory body or entity that authorizes cloud service offerings for use by their respective governmental agencies or regulated industries.”*
* Reviewed the “Cloud Topology” section of the Guidance Doc
  + Brandon H has a photo of the whiteboard drawing of the rough cloud topology from the in-person workshop. This will be incorporated into the Guidance Doc at a later date.
* Modified Guidance Document section “Cloud Equivalence Considerations” as follows:
  + *“In general, products must be tested individually on each desired cloud service offering.*

*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. CC Scheme policy may define acceptance criteria.”*

* Reviewed Guidance Document section “CPU Equivalency”
  + Discussion on whether the CAVP IG is still relevant despite it’s mature age
  + NIAP Policy 5 is the most current source of information, however Jade S advised that NIAP has resources actively working on bringing requirements in sync between NIAP & CAVP program.
  + “CPU Equivalency” Section modified as follows:  
    “*Applicable guidance shall be followed when labeling Operational Environments. Such as:*

*For a Type 1 (or native) hypervisor, where the hypervisor runs directly on the hardware, the OE listing shall include the guest OS, hypervisor, and processor using the following format: “Guest OS on hypervisor on Processor.” An example is “Microsoft Windows 11 on VMWare ESXi 7.0 on Intel Xeon W (Rocket Lake).”*

*For a Type 2 (or hosted) hypervisor, where the hypervisor runs on a host operating system (OS), the OE listing shall include the guest OS, hypervisor, host OS, and processor using the following format: “Guest OS on hypervisor on Host OS on Processor.” An example is “Microsoft Windows 11 on Parallels Desktop 17 on macOS Monterey on Intel Core i7 (Kaby Lake).”*

*Algorithm tests may also be performed using containers. The OE listing shall include the container, runtime, host OS, and processor using the following format: “container on runtime on host OS on processor.” An example is “Ubuntu 20.04 Docker Image on Docker Engine 20 on Ubuntu 20.04 on Intel Xeon W (Rocket Lake).”*

*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.”*

**Questions/Follow-ups:**

**~**

***End of Meeting – Adjourned 0901 PDT***