7:28 AM PDT 2022-09-07

**Call to Order:** 0732

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 15

**Next Meeting:** September 21st, 2022

**Highlights:**

~

**Old Business:**

~

**New Business:**

1. ***Discussion around what might constitute a non-trusted cloud service provider*** 
   * Geographic locations of hosting, political/governmental regulation & control of CSP’s
   * Some rumors last week with tiktok and customer data being exposed by an open bucket on the Alibaba cloud.
2. ***Discussion on words and concepts that provide or describe “trust”***
3. ***Discussion around “Trusted Provider” vs “Trusted Platform”***
   * “A trusted provider provides a trusted platform”
   * Trusted Provider:
     + Proven success
     + Acceptable gov cloud risk mitigation framework such as FedRamp, C5, SecNum, etc.
     + Visibility into when security relevant changes will happen. For example updating to TLS 1.3 – SOC2 may cover.
     + Data privacy policies need to be available
   * Trusted Platform:
     + CC certificate for O/S, V/M, GPCP? Need to define what is an acceptable delay
     + FIPS algorithm validation certs (US/Can) Need to define what is an acceptable delay.
     + Additional higher level frameworks such as IL5, IL6 would be a plus
     + Cloud providers update underlying systems frequently.
4. ***Discussion on drafting a paragraph on what a Trusted Platform includes as it relates to CC in the Cloud?***
   * “A trusted platforms definition depends on the protection profile(s) being evaluated against. A platform provides the operating environment for a given TOE that typically meets the requirements for a particular evaluated configuration. Components of a platform may include: an operating system, virtualization hypervisor, various switches and hardware needed to run the software. Some technology won’t need all of the components listed above because for example an O/S is contained in an appliance such as a network device. “
   * “How do platforms become trusted platforms. The CC in the Cloud TWG suggests the following minimum requirements would be needed:
     + A common criteria certificate for each relevant component in the platform being utilized by the TOE.”
     + (Look to the ESR for potential guidance on this)
   * “For example, the NDcPP depends on the O/S, the virtualization provider and/or the underlying hardware. As opposed to the software App cPP utilizes the O/S for most of its security functionality.”

**Questions/Follow-ups:**

* What items in the platform stack need CC? Does hardware (eg. Servers, networking) need to be evaluated?
  + Only include the relevant platform? The layers being utilized by the TOE?
* Data Separation/Segregation strategies (how is cloud tenant data isolated?)

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