Lessons Learned from the 90B Pre-Reviews

Alex Calis

April 28, 2021

Main Technical Issues Discovered (1/5)

- Discrepancies on how an assessment demonstrates compliance to 90B.
  - How does it map to each 90B “shall” statement?
  - Same thing for IGs 7.18 (D.J for FIPS 140-3) and 7.19 (D.K for FIPS 140-3).

Main Technical Issues Discovered (2/5)

- Some reports had minimal justification on the H_{submitter} estimate.

- Others did not explicitly indicate what the primary noise source was, or if they were physical or non-physical.

Main Technical Issues Discovered (3/5)

- Some made no assumptions on the entropy source to help shape the analysis.
- Lack of justification on if the output samples are considered independent or dependent.

Main Technical Issues Discovered (4/5)

- The report was not sufficiently self-contained.
- Poor references.
- Lack of references.

Main Technical Issues Discovered (5/5)

- Lack of information on how the entropy source met the restart requirements.

- Missing how was the noise source data was collected.

Overall

- There were a lot of great information within these assessments.

- Learning experience for everyone involved.

- Without a template or baseline checklist, we cannot expect uniform submissions at this time.