File 20100513.1000: Notes from 5.0 certification report telecon (classified) in the YF scif this morning, 0800:

Attending were (incomplete list): NSA pen test team, DNI, Audrey's (Autry?) team, DNI CAT, Phyllis—Pen Test lead who runs the show, Dennis Bowden, Dan Griffin, Hawk, Kevin Miller, myself, Ian McGlothlin, Paul Ozura, Orville Brown, Geoff M.

The purpose of the telecon was to go over LM responses to findings and NSA response to LM's response.

Emily: some of LM's responses look to the pen test team like they are planning to introduce new functionality.

NSA pen test team believes findings should be fixed; LM does not want to fix all of them; we are at a stand-still. (I think this was Phyllis.)

The test director, who is DNI CAT, also believes findings should be fixed.

Either they need to be fixed, or there needs to be some other mitigation, or the certifier (STRATCOM) needs to accept the risk.

Fix-before-deploy?

LM will provide all CRs to the regression test team so they know exactly what changes are being made to the UCDMO baseline.

Next meeting Thursday, same time same place.

If new functionality is introduced, it is no longer regression test but delta test, and without additional time. This is distressing to the test team.

Installation and testing schedule slipping one week to the right.

Call ended 0941. Subsequent call with Programme Office began immediately after:

Phyllis [NSA pen test] is complaining even now that RHR in RM does not deliver what is promised to customers. She says RM advertises that it blocks malware in (for example) JPEGs but that it really does not. The developer counters that no automated guard can inspect opaque binary data structures (cf. the steganography problem) and that the developer considers the risk unacceptably high, hence imposes *reliable* human review with trained and experienced operators. Phyllis complains that WinDDS does not come with any actual review tools; the developer replies that it's by design—the particular review tools installed are always those that the accreditor specified. LM maintains that what is being certified is the RHR framework, but the accreditor must define what actual tools are needed for a particular operational site; e.g., antivirus, PuriFile, IC Clear.

The developer expects to receive Charleston's report next Tuesday now.

Russ Savage: Phyllis has always hated RM since day 1. She will always mark WinDDS as a high risk.

5.0zd will come after Thursday. The chances of Kori Phillips not finding *anything* in the build are almost nil, after all.

References