File 20100715.0800: Notes from RM 5.0 CT&E hotwash telecon this morning, 1000–1100 EDT time (0800 MDT):

Present on the call were Kim Frey, Olav Kjono, Kevin Miller, Joe Loughry, Dan Griffin, Larry Brown, Rob Drake, Don Flint, Dave Oshman, Emely Martinez, Corinne Castanza, Phyllis Lee, Charissa Robinson, and Larry Sampson.

Phyllis began by complimenting LM for being responsive, but expressed frustration that the pen testers have been unable to finish all the tests they want to run, because they keep running into breakages. Testing stops while the developer fixes a problem, then testing picks up again. The pen testers are frustrated that previously identified findings are being found not to have been fixed, and new findings are found besides. It is slowing down testing.

LM replied that in the TOE test scenario set up for the test labs to operate in, there are numerous factors that differ from the real world. In actual installations, a running configuration is very specific and tuned to do exactly what is needed. No matter how much the pen test team would like the system they test to reflect the real world, the exigencies of testing enforce an artificial environment. The developer strives to give testers an opportunity to perform significant and meaningful tests on the full scope of functionality of the system, but testing some features in combination is neither meaningful nor realistic.

NSA wants another week for regression testing. They will not accept any more code changes for a week. At the end of that week, the developer will provide a fix, and then NSA will determine what needs to be re-tested. Phyllis believes that the additional week of government regression testing will not adversely affect the schedule.

This was followed by a classified discussion of robustness and the WIN-T, TACELINT, and VMF formats.

Rob Drake is on the line.

[more classified discussion elided]

Emely: The pen testers not been able to look at key functionality because of the problems that keep cropping up. Look at the history: CT&E started back in March. Since CT&E began, the test team has never been able to get the entire system up and running. They spent a week trying to install, debugging, changing mags on the fly. Not to fault Lockheed Martin—it was a very aggressive schedule. But every time the team starts trying to test, something else breaks. LM has always been very responsive. But every time the testers try to test, it's back and forth, back and forth.

[classified discussion of stability]

Kevin Miller: there is only a single issue that has been found but not fixed, and that is only because we were unable to reproduce it until recently. We keep hearing generalities about a large number of unfixed issues, but there is only one problem that has not been fixed yet.

NSA replied that repeated test stoppages have kept the pen testers from getting through all the tests they wanted to run.

[classified discussion of SNMP, DFCF, data link]

Dennis Bowden: The decision will be documented in the Cross Domain Appendix. The feature is not enabled by default. Sites that want to use it will be advised of the elevated risk.

Phyllis said that maybe we had better go back and look at older versions of RM on TSOL 8 to see if those have similar risks. We have new information now.

Rob Drake asked: How many weeks of delay of ST&E at STRATCOM, which currently starts in August, are we talking about?

Corinne: three weeks is the best case scenario.

Rob Drake: I want to talk to the other accreditors. Personally, I am still inclined to go forward on August 2nd and fix things later. My own risk assessment is that the risk is low.

Corinne: If you are willing to accept the risk based on the test results you have been given so far, which is not all the testing that NSA wanted to perform, then...

UCDMO: The agreement at the beginning was that Rob Drake would make the decision for this iteration. We should hold off the baseline until we get a common agreement.

Rob Drake: If, when we do ST&E at STRATCOM, we find any findings, then we should fix those and put the fixes into the baseline. I am still pressing to stay to the present schedule.

[Editorial note: Kevin explained to me that Rob Drake's responsibility and inclination are to get TSABI done; he is less concerned about SABI. Not sure how this will affect the certification date.]

SSC Charleston described a hypothetical situation with remote management. LM maintains it could not happen in the field. SSC Charleston will send the developer a set of unclassified files containing test

data.

Next hotwash is scheduled for 1000 EDT on 22nd July 2010. Call ended 1100 EDT.

LM's Takeaway points:

1. One more week is needed for NSA pen testers before a new code drop. After that, NSA will need one week additional for regression testing.

2. NSA pen testers are frustrated that they cannot perform testing non-stop without encountering issues. (This is where the original plan to have an RM engineer on-site during the entire test event would have been very beneficial.)

3. Phyllis used harsh words. It is crucial to recognize, however, that the NSA testers are looking at a completely unrealistic configuration. Their test system is a Swiss Army knife. It has every bell and whistle turned on, things that would not ordinarily be used in combination. Operational installations of RM are never configured that way.

4. Rob Drake is pushing strongly to stick to the original schedule.

5. Data link risk will be documented, it will be installed only where necessary, and the risk communicated to those sites.

6. The developer will look into Charleston's additional issues with the test data they will send. Expect that the fix will NOT require any software changes, only configuration parameter changes.

7. LM will likely send Kori Phillips to NSA next week for support.

8. After many sharp remarks from Phyllis, in the end she seems to be OK with rating certain things as high risk and moving on as long as they are documented. Need to ensure that only those specific items are rated poorly, and not the whole guard.

References