File 20101001.0830: Notes from RM 5.0 CT&E hotwash this morning:

Present on the call were Larry Sampson, Kevin Miller, Joe Loughry, Craig Christensen, Dennis Bowden, J. ? for USSTRATCOM Western Region, Dave Oshman (NSA), Don Flint, Orville Brown, Charissa Robinson, and Corinne Castanza. Dan Griffin is away because of a death in his family; Dennis Bowden represents the government Programme Office.

The meeting was supposed to discuss Version 5 of the POA&M, but most of the government agency participants said they had not received it yet. The agenda of the meeting was to discuss Corinne's and Charissa's final test reports.

Dennis Bowden noted that he is waiting for an accreditation letter from Dan as soon as he gets back from travel. The accreditation letter, representing one ATO at the SABI or TSABI level, is a required component of the Phase III ticket exit criteria.

Version 5 of the POA&M includes all DIA, DNI and CDTAB concerns. As was discussed by some participants at the CSTG last week, the POA&M is intended to be a living document, updated with new information about threats and mititgations as they are developed over years. Speaking for Dan Griffin, Dennis Bowden said that the 5.01 patch will now contain fixes for all findings dentified in the POA&M as requiring non-procedural mitigations. It will be necessary for LM and RM PMO together to spend the next few weeks determining what kinds of regression testing are required, then what kinds of testing will be required from external agencies. Early next week, Dennis Bowden will talk with Dan Griffin and LM.

The developer is working with an excellent new document written by Corinne that explains the RBAC problem. It will take several weeks to make all the necessary changes, but the effort is under way already. Corinne praised the developer for being so proactive.

[not to include in weekly activity report] The output_guard process now runs as a different userid than rmuser, with unneeded privileges now removed from rmuser.]

Dennis Bowden said there are four customers that really need 5.0 right away. He asked if it would be possible to work with the CDSOs to get those four briefed at the October CDTAB, as the operational need is urgent. Charissa said she met with Paul Ozura earlier in the week; do those sites have Phase I tickets in place? Answer: yes; all they need is the Cross Domain Appendix to complete Phase II. As soon as that arrives, they will proceed to Phase III. The CDA template is done now. Charissa asked whether the four customers are upgrades, or new installations? Answer: new installations. Dave Oshman stated that it is really the CDSOs that need to push in order to get those sites slated for CDTAB.

As was discussed by several of the participants at CSTG, it has been a long, hard slog to get through RM 5.0 CT&E, and it may be unnecessary to hold any more of these hotwash telecons.

Orville Brown and Corinne discussed a technical question about the label_encodings and exec_attr files in the POA&M. The upshot of it was that if certain capabilities are operationally necessary, then they are, and Corinne will simply have to document the risk assessment on them. She is OK with that as long as it is documented.

Larry Sampson then said that from the UCDMO perspective, until the mid-October time frame, the participants will leave it open to have as-needed classified or unclassified telecons. Corinne noted that feedback from NSA I173 is that they will have their final pen test report by November. Dennis Bowden asked, as you prepare to brief the next CDTAB, please consider inviting IV&V. He talked with Glenn Learn at CSTG last week, and understands now better why the developers are not let in.

Call ended 0830.

After hanging up, the developers discussed amongst themselves. Kevin complained that they never read anything we send. Ian noted that 95% of the government people claimed never to have received the Version 5 POA&M. Don blew Corinne's cover when he said 'it's in the folder'.

Kevin said Corinne wrote a great paper on the root role problem—the root role is unnecessary on an operational system. Kevin noted that the proposed solution will necessitate more telephone support time; every time the site wants to use root it will be necessary to change the user_attr file and reboot; this will take a *good* engineer at least thirty minutes extra on the phone. They are considering adding a button to do it, but from Corinne's perspective, it's another attack vector.

The UCDMO Baseline List was not published today (1st October), but that is not surprising; sometimes it takes them a few days. It is on the unclas internet; I am watching for its appearance. The developer expects to see RM 5.0 listed, but only the first TORA.

After the telecon, Craig Christensen told me this morning that he does not have the new contract for Probabilistic Redaction yet for FY 2011, so he may need to shunt me off for a few hours. I told him that Jeff Dutoit already gave me a different charge number to work on the DARPA RFI proposal, so that is what I am working on for the next 12 hours. It is due today. Jeff will get it *late* today. Craig says the PR contract will be updated by Monday.

References