File 20100902.0900: Notes from RM 5.0 CT&E telecon this morning:

Present on the call were Kevin Miller, myself, Don Flint, Rob Drake, Dennis Bowden, Larry Sampson (moderating), Jake Randall, Charissa Robinson, Dan Nichols, Dave Oshman, Dan Griffin, Olav Kjono, and Lisa Ackerman. Rob Drake began with a review of his preliminary ST&E report and POA&M validation, highlighting three categories of CT&E items: (a) items that can be closed, (b) items that he wants to give another look, and (c) items that remain open but are covered by the POA&M mitigation plan. From the validation report, fifteen or so category A items have been closed entirely; these vulnerabilities no longer exist. Of the items in category C that remain open, all are addressed by the POA&M. Category B lists the failed security controls that he wants to look at again. Some of these are instances where the system is working as designed. Others are vulnerabilities that cannot be fixed for technical reasons. Either way, they are not findings; according to him, something that cannot be validated cannot be a finding.

Regarding the ST&E and (STRATCOM) pen test reports, UCDMO requested that the two reports not be combined. To make information more clear for the baseline, the pen test report will be divided into two parts: CDS-relevant findings and site-relevant findings.

Dennis Bowden asked about a certification/CT&E letter. Rob Drake intends to put out an accreditation letter soon. Each agency, e.g., DIA, will issue its own accreditation letter. These do not indicate a type accreditation, merely that RM 5.0 has been tested and certified in one instance. The letter is not site specific. The generic accreditation letter is intended to feed into every site's Body of Evidence (BOE). For its BOE, for example, DIA will be using the old SSAA, and other pieces. Once DIA CIO leads with the letter, then DSAWG looks at the BOE, plus their own BOE, considers everything, and decides whether to put the CDS on the baseline. DSAWG needs one ATO as part of a BOE to go forward with placing RM 5.0 on the baseline. There is an interim (three-month) ATO at STRATCOM currently because there is not yet a full BOE. The 800-53 report is not yet finalised; that is the only thing holding the accreditors back from issuing a full three-year ATO.

There followed a discussion amongst Dennis Bowden, Dan Nichols, and Charissa Robinson about whether the BOE should include the long form SSAA or the new SSP. Answer: UCDMO will accept either SSAA or SSP; there is no need to duplicate effort by preparing both. In that case, Dennis Bowden will continue polishing the long form SSAA. Mr Bowden asked if the SharePoint site has been set up yet for collating BOE documents; Mr Nichols stated that UCDMO needs to receive the documents themselves, not a pointer to a site. The reasoning is that UCDMO do not publish the BOE, because they are not UCDMO's documents to distribute. UCDMO cannot be the repository for collecting documents. Nevertheless, UCDMO insists that it receive BOE documents directly from the government, i.e., Dan Griffin. Dennis Bowden may prepare it for Dan Griffin but the PMO must transmit the BOE to UCDMO.

Charissa Robinson asked about having a Lockheed Martin engineer at the CDTAB on 21st September. CDTAB members will likely be very curious and will be asking lots of questions about internal processes within the guard, how those processes communicate, use of privilege in the OS, and so on. It would be highly beneficial to have an engineer available who is familiar with the internals of the software, not just with the test procedures. This resulted in some discussion; it is unusual to have developer representation at CDTAB, but the present situation is unusual, giving that the certifiers are learning the a new process as they go along. The developer agreed to provide an engineer; IV&V will also send representation along.

Rob Drake promised that the ST&E test report will be available next week. He is doing housekeeping details on it now. It will be delivered by 10th September. Larry Sampson will send out a matrix to all participants detailing all items needed to close this thing out. Goal is for Dan Griffin to have all the documents he needs to do a baseline submission towards the end of the month. Three to five documents make up the BOE: the accreditation letter, CAT report, test report, POA&M, and UCDMO tick list. Dennis Bowden is working from the January 2009 UCDMO tick list. Larry Sampson will provide an updated template for the RM 5.0 fact sheet; the fact sheet is not part of the BOE, but is distributed by UCDMO to the community.

Version 4 of the POA&M (pronounced 'poem') uses the following colour coding: green indicates findings that were corrected by a software change; light green indicates findings that were corrected by a procedural or configuration change (no software change); orange indicates findings that will be addressed by an immediate post-5.0 patch; blue indicates findings that are deferred for a future fix; grey indicates no planned fix: findings that have been ruled invalid or out-of-scope of this test.

Charissa Robinson mentioned that her organisation plans to do multiple target-of-risk assessments: one for the CDS alone, one for the CDS with remote management, and so on, so that sites can use the one most appropriate to their situation.

The pen test folks never did show up today. At the end of the meeting, Rob Drake noted that one of his Category III findings (non-critical) addresses a lot of 800-53 organisational controls—covering, e.g., power supply capacity sizing, environmental specifications, and so on—have been left open by the current CT&E and ST&E procedures. These questions are not, in his experience, an ST&E event; they are a site event. Probably subsumed at STRATCOM by the existence of a SCIF and TEMPEST letter, but at the moment they are still open, and need to be closed. All a part of learning and debugging the new process.

There will be a hotwash telecon next week, probably Thursday. ST&E is completely done. A few housekeeping tasks remain, open action issues that are the accreditor's responsibility, but not the developer, PMO, or the site.

References