File 20111109.0834: Notes from Raytheon TCS C&A webinar, presented by Steve Welke.

Raytheon TCS makes the High Speed Guard, Trusted Gateway System, Trusted Thin Client, and Trusted Virtual Environment. See the UCDMO basline list for the whole list.

TCS webcasts about what they have learnt and would be useful to pass along to the community. Today: Cross Domain C&A processes.

- DoD: uses SABI
- IC: uses TSABI

There are current community initatives to standardise CDS C&A processes.

All C&A efforts have:

- Roles
- Activities
- Documents

Why do we do C&A? Because systems are put into place to accomplish missions.

Risk equation. Residual risks that remain must be assessed and accepted before operational use.

Courtroom analogy: the DAA is the judge. The certification authority is the jury. The C&A documentation is the defence lawyers.

Recent changes are happening throughout the community:

- DITSCAP moved to DIACAP in DoD
- DCID 6/3 moved to ICD 503 in IC
- NIST (based on FISMA) in civilian world

Three communities, all doing C&A their own way.

Components of C&A: every C&A process has these three components:

- Roles—essentially the same in every process
- Activities—essentially the same in every process, divided into the same four phases:
  1. Preparation (the longest phase)
  2. Testing
  3. Approval or accreditation
  4. Deltas, ongoing maintenance
- Documents—the content is always the same, but the form of the BOE varies.

THIS IS IMPORTANT!

The C&A process acts as a double check on what a good software engineering process would already have done, with maybe a little more attention to security. If you don't have a good software engineering process up front, the C&A process will be painful.

SEE ABOVE.

SABI: created by NSA and DISA, now being developed by the CJCS.

- Roles:
  - NSA
  - CDTAB
  - DSAWG
- Activities:
  - CT&E (SR 1–9)

  - ST&E
  - Risk assessment (using the RDAC)

- Documents:
  - Cross Domain Appendix (CDA). This is where the SABI group got it right. For CDS, the CDA is just an appendix atop the usual BOE. It simplifies things.

SABI Roles: (see Mr Welke's slide package for the diagram with all the numbered arrows) To begin, send your Phase 1 C&A package to your CDSO, who sends it to CCAO. CCAO sends it to CDSAP, who puts it on the agenda of the Community Jury. If they're OK with it, then CCAO issues a SABI ticket number and assigns a SSES and C&A facilitator. Then NSA gets involved. NSA does the *lab based* CT&E testing. (NSA labs are fee-for-service, take 9–12 months, and cost 0.5 to 1.0 million dollars.)

Phase 2: Then the RDAC group gets involved, send their results to CDTAB, who pass their recommendation to the DSAWG.

If the DSAWG approves, then the site does ST&E in Phase 3 CDA. It loops again through RDAC, CDTAB, and DSAWG to evaluate the results of ST&E (the first go-around was to evaluate the results of CT&E), and finally back to CCAO in Step 12.

Minimum amount of time to get through the process: note that each group meets once a month; in the morning they are CDTAB, in the afternoon the same people are DSAWG. The requirement to go through the boards serially, and the fact that they only meet once a month, is one of the reasons the process takes a minimum duration of many months.

In reality, SABI takes 6–9 months for a CDS that has *already* been through NSA lab testing. If it's a brand-new CDS that has bever been tested before, then 2–2.5 years and 0.5 to a million dollars. Once a CDS has been through NSA lab CT&E testing once, it never has to do it again. Everyone accepts the results.

Components of CDA.

Now, let's look at TSABI.

- ICD 503 is the NIST approach to C&A
- Based on Risk Management Framework (RMF)
- CNSS and IC specific guidelines added only when needed.

Roles: DIA, PAA, Certification Test Authority (CTA) and CAT.

Activities:

- Beta I is lab-based
- Beta II is site testing

Under ICD 503, the Beta I and Beta II are *renamed* CT&E and ST&E.

Documents: short form SSAA/SSP.

Differences: the DNI CAT does not cost you anything in TSABI. They perform the same lab based testing as NSA, but not a fee for service arrangement.

Timing: TSABI CDS C&A takes about three months; another month or so if lab based testing required.

TSABI documents: the SSAA/SSP is an executive summary of a bunch of appendices.

Current community initatives to standardize CDS C&A:

- NIST: Risk Management Framework (RMF)
- UCDMO:
  - CDIF
  - CD baseline
  - CD Security Control Overlay

NIST RMF:

- ‘categorise, select, implement’ in Phase 1.
- ‘assess’ in Phase 2.
- ‘authorise’ in Phase 3.
- ‘monitor’ in Phase 4.

‘C&A’ will be renamed ‘A&A’ (new terminology).

UCDMO: CDIF effort, Cross Domain Security Control (CDSC) Overlay.

CDSE Memo was signed 11th October 2011. CDIF is a concept and has not been approved or implemented yet to date.

Email `RKonosky@TrustedCS.com` for the slides.

References