File 20110407.1532: Notes from C&A webinar:

TCS was acquired by Raytheon recently. Originally developed the DoDIIS Trusted Workstation (DTW). Presenter: Steve Welke.

Three C&A approaches, one in DoD, one in IC, and one civilian. In the DoD, C&A moved from DITSCAP to DIACAP. In the IC, from DCID 6/3 to ICD 503. In the civilian world, NIST C&A is based on FISMA. There is an attempt to bring the three together under DNI/CNSS.

There are two C&A]emphprocesses for CDS: SABI for DoD and TSABI for IC, both now under UCDMO.

C&A or Security Authorisation?

Every C&A effort consists of three components: roles, activities and documents.

Why C&A? Systems are composed of resources, which have vulnerabilities and (maybe) associated threats. A threat combined with a vulnerability results in a risk. Risks motivate security requirements and security controls. The residual risks that remain must be formally accepted before ATO. If you have no threat, you have no risk. If you have no vulnerabilities, then there is no risk.

C&A is an informed approach to managing risk. It consists of evaluation, certification and accreditation. Evaluation of a product, certification of a system, and accreditation of an installation in an operational environment. Certification includes the people, processes and procedures that surround the technology when making the risk decision.

By analogy, in a courtroom, the lawyers make an argument to the jury, the jury makes a recommendation to the judge, and the judge makes the decision.

What matters to your particular DAA? He or she is the most important person in the C&A process. Certifiers are more technically knowledgeable than most DAAs. They make a recommendation to the DAA.

Need for common C&A process. All the services had their own. The first commonality was within communities: DoD, IC. The civilian C&A process was created after the FISMA act (it required NIST to create one).

DNI and the Committee on National Security Systems (CNSS) are trying to bring all three of DoD, IC and civilian C&A *approaches* together. This is separate from the C&A world.

Roles, activities and documents.

For SABI, NSA's board of certifiers is CDTAB; their board of accreditors is the DSAWG.

Welke praises the Cross Domain Appendix (CDA) as the one place SABI really got it right.

Beta I and Beta II were terminology that came from DCID 6/3?

References