File 20110330.0928: Notes from Raytheon C&A webcast 0900 today. I missed the first half, but the slides and audio are supposed to be available on `http://www.trustedcs.com/resources/webcasts.html` soon. This was an excellent webcast, and I look forward to getting the material for closer and repeated study. It was very information-dense.

Differences between DITSCAP and DIACAP: DoD 8500.2 security controls, incorporated deltas.

DIACAP moving from 8500.2 to NIST SP 800-53 in DoD. ICD 503 replacing DCID 6/3 in IC. ICD 503 supercedes DCID 6/3 and 6/5 ('Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI)'). It is also the NIST approach to C&A.

CNSS adds a few requirements atop ICD 503.

The chain starts with NIST SP 800-39 as the keystone document. It goes from there to 800-37 Risk Management Framework, 800-53 Security Controls; 800-53A is a process for assessing, and the new one, 800-137 is a policy for continuous monitoring.

The term 'C&A' is going away soon, to be replaced by Assessment and Authorisation (A&A). C&A implies a finality that led people in the past to try to pick up an accredited system and put it down someplace else. The new name, A&A, correctly reflects a *security authorisation process*.

The same author has a CDS C&A process webinar coming up. I registered for it immediately.

SABI and TSABI have different names for the same concept. What SABI calls CT&E, TSABI calls Beta 1. What SABI calls ST&E, TSABI calls Beta 2.

The UCDMO mission is to bring SABI and TSABI together as much as possible. The UCDMO baseline is the biggest thing that UCDMO brings out.

His definition of C&A is People, Processes, and Technology in a Particular Place.

Discussion of reciprocity. Reciprocity means that DoD will not re-test what IC has already tested to a higher standard. It does not mean that just because something has been tested in one place, it can be used in another place without testing.

References