

File 20110408.0442: Weekly activity report 0183:

weekly activity report 183 (loughry)

Joe Loughry

Sent: 08 April 2011 04:42

To: Niki Trigoni; Andrew Martin; Joanna Ashbourn

Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;

chip.auten@comcast.net; edloughry@aol.com; diane@dldrncs.com;

Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20110407.2013 (GMT-7) sequence no. 0183, week 8+4 HT

Research: I am working on the section in Chapter 1 on the justification for current C&A practices in the defence and IC as they emerged from 5200.28-STD. The approach I am taking is to disregard FISMA for the time being; if present trends continue, civil and commercial C&A will continue to move in the direction of the NIST 800-series risk management framework and security controls, subsuming more and more of the CC v.3's SFRs and SARs and then displacing it in the manner of TCP/IP and the OSI model. I must compare ISO 270xx to NIST 8xx and decide if there is any chance of a direct USA--EUR mapping. The preceding question was the first of two digressions this week that, while time-consuming, were necessary to follow up on. The second was a methodological question relating to Chapter 3. Returning again to primary sources, it seems clear that despite Glaser and Strauss's (1967) low opinion, expressed in footnotes, of Melville Dalton's research ethics in the 1959 book *Men Who Manage*, it was exactly that work---more than any other in their list of references---that drove the publication of *Grounded Theory* into the literature. Dalton's method is more closely aligned with the form of the source data of the R', R'' and R-zero case studies than either Glaser's or Strauss's. Consequently, I describe a methodology less close to that described in Bryant and Charmaz (2010) but more suitable for the aim of the present study. I am acutely conscious, however, of the need to get chapters down on paper in time for Easter in only a week or so.

Miscellaneous: I revised my write-up on SSD forensics-friendly design features for the capture manager's proposal on Friday, and obtained an interesting list of application areas in which R and R'' have been installed in the field from the developer's CM representative. I read two presentations and listened to a recorded lecture all on CNSS refinements to the NIST approach to C&A. I re-read the updated DoD 3305.13-M in an attempt to figure out how it could possibly relate to 8501.01-M and hence to the continuous monitoring phase of C&A; I finally figured it out: the 'Security Professional Educational Development' (SPD) programme establishes accreditation guidance and procedures for trainers of 8570.01-M IAT, IAM and CND personnel. It applies to both the DoD and civilian IC workforces. What is not clear is whether it applies to DAAs and DAA reps; I am trying to find out.

I owe another quarterly progress report to my Air Force funding sponsor; that report is late because I spent the entire weekend doing taxes. Status: about to begin skimming (cursorily) old daily logs from 2004--5 in an attempt to estimate the amount of GT work in R' for the methodology in Section 3.3. Due date for COS application: 18th April.

Joe Loughry

Doctoral student in the Computing Laboratory,  
St Cross College, Oxford

End of WAR 0183.

## References