File 20090425.1720: After-action report: ISSEP examination, London. I think I was not successful. The exam was three hours, 150 questions, and I ran out of time checking my answers. I made a costly mistake by not recording any answers on the № 2 scantron sheet until the very end, and I ran out of time transferring the answers to the scantron sheet after only about 68 answers. Therefore, even though I had the answers, I failed to record all of them and thereby did not complete the exam. I don't think I passed.

The examination rules require candidates writing the examination to stop writing instantly at the end of three hours, close the examination book and not make another mark on the answer sheet. I followed the rules, even though it would have been preferable to keep writing. I was scrupulously honest.

Preparation was adequate; it was a very difficult exam, 150 questions and only three hours, and I ran out of time. However, I knew the material and I think I can pass it the next time, simply by keeping in mind the time limit and working a little bit faster. I had worked out the answers to about 130 questions (another twenty I kept going back to—that's why I ran out of time); I believe I would have passed the examination if I'd had seven more minutes to finish filling in bubbles on the answer sheet. However, it counts for precisely nothing that I knew the answers, or even had circled them all clearly in the exam booklet. Only answers recorded on the answer sheet are counted. Andrea says I should wait for the score report and see if I passed it. anyway. I will, although I don't think so. I think I would have passed fine if I'd just recorded all the answers on the answer sheet.

Topics on the exam that surprised me included DIACAP (nothing at all on DITSCAP), which changes the names of some of the roles of people, and that tripped me up. There was a question about FIPS 140-2 that asked what combination of concepts it deals with, including trusted operating systems, cryptographic algorithms, tamper resistance, access control, authentication (authentication? To a cryptographic module? Well. . . maybe.), key management, key distribution, and keys. I want to go back and find out whether it was 'tamper resistance' or 'trusted operating systems' that they wanted. I think it was tamper resistance.

**Update:** Yes, the question was referring to authentication to a cryptographic module [2, p. F-53].

There was quite a bit of memorisation of US Public Law numbers, privacy act of 1974, Computer Security Act of 1987, and who requires privacy policy statements to be emitted by web servers and who sets controls for personal information on US government systems. Like HIPAA, I never paid much attention to those. There was a question about cookies, and who has to approve their use on US government computers. (Who cares? Well, the ISSEP exam people do.) So review Public Laws and privacy act and unclassified federal systems and all that jazz.

There were a number of very poorly worded questions, one spelling error ('principle' for 'principal'), a couple of subtle red herrings and one or two questions where none of the answers seemed right, or multiple ones seemed 'best'.

Mostly, I want to review people's rôles, especially the *abbreviations* for roles used in DIACAP. Review the phases of DIACAP and how they differ from the older phase names used in DITSCAP. Look for the official (ISC)$^2$ study guide, since [1] is clearly out of date now. Consider a one-day class for review, if offerred. Look a little closer at FIPS 140-2, and at IEEE 1220, and at OMB Circular A-130. Also, who has **FINAL** oversight responsibility for cryptographic algorithms used for integrity in classified systems: NSA or NIST? Also, what CIOs are useful for, and what Programme Managers (PM) are useful for, and what Systems Engineering plans contain. There was one annoying question that seemed to have multiple correct answers, on what tool is best used for assigning resources and tasks: PERT, Gantt, or WBS.

Review the management side of things a little more, including SOW and WBS—what each contains, how they're different, and what each is useful for.

Next tasks:

- Record any other thoughts on this that come up in the next few hours or days.
- Check dates of next examination.
- For the Table of Contents due Wednesday, focus on the C&A chapter. Make it a disguised ISSEP review. That way I can keep the information current, develop in writing precisely the weak areas, and get a thesis chapter done at the same time.
- Back to work on thesis now.

# References

[1] Susan Hansche. *The Official (ISC)$^2$ Study Guide for the Information System Security Engineering Professional (ISSEP) Exam.* Taylor & Francis Ltd, 2005.

[2] U.S. Department of Commerce, National Institute of Standards and Technology. *NIST Special Publication 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*, June 2009. Final Public Draft.