File 20100122.1121: Notes from LM-VTIS call this morning on DOD 8570.1 compliance within Lockheed Martin:

Mike Nance, LM Fellow

Here is more updated information on DOD 8570.1 courtesy of the best available knowledge of SMEs within Lockheed Martin as of January 2010:

1. There is about to be an update to 8570.1 in the next month or so. It will add $(ISC)^2$'s CAP (C&A) to the list of acceptable certifications for a low or mid-level employee in a management role. CSSLP (software security life cycle) will be added soon for developers to focus on secure coding skills. I think CSSLP might be extremely useful to us for all developers who do not already have a CISSP.

2. The other big surprise is the addition of Certified Ethical Hacker (CEH). It looks like 8570.1 intends it for CND operations folks, unfortunately not something we do a lot of. However, I think we could argue that installers who have any involvement in ST&E would benefit from CEH, possibly in addition to CAP. (I think developers and mag writers should have CSSLP at minimum).

3. Another perspective on that square matrix:

   - Techs:
     - IAT Level I works in a server farm, builds machines, but doesn't know networks at all.
     - IAT Level II knows everything Level I does, plus understands TCP/IP networking.
     - IAT Level III knows everything in the first two levels, must be a US citizen, and can touch enclave data.
   - Managers:
     - IAM Level I manages the Computing Environment (CE), i.e. server farms.
     - IAM Level II manages the Network Environment (NE).
     - IAM Level III manages the enclave environment, i.e., intelligence or customer data.
   - Designers:
     - IASAE is a designer, either systems engineer or software developer. IASAE Level I writes code that runs in a server farm. IASAE Level II knows everything an IASAE Level I knows and designs applications that depend heavily on network behaviour. IASAE Level III knows everything an IASAE Level I and II knows, plus interfaces with senior government people and accreditors.
   - CND (this is the new layer):
     - CND monitors the enterprise and responds to attack. I think of them like shift-based NOC personnel. CND does not have levels; it has CND Analyst, CND Support, CND Reporter, CND Auditor, and CND-SP Manager.

DEADLINES: the most current guidance is to have 100% certified IAT and IAM by end of CY 2010 (this was changed from FY to CY so the deadline is now December 2010, not September 2010). Some DAAs and some contracts are being hard-assed about it, however.

100% by end of this calendar year. No later.

Overall DoD was around 40% certified as of 30 Sept 2009. They will likely still be short of their 70% goal.

I emailed Michael H. Nance to thank him for his informative presentation.

References