File 20110616.1435: Notes from Kevin Miller's report on the 2011 Lockheed Martin IA Conference, 24–25 May 2011.

There are two RMs in the JSF programme. One is used for logistics information, because it cannot be shared freely with international partners. The other protects flight test data.

DUTCH is a programme aimed at protecting the hardware/firmware of a platform. Uses Intel's SMM capability? Patches, host-based IPS, firewall, anti-virus, configured to STIG. TPM, Intel approved BIOS vendors, authenticated code, measured launch environment. All these have been hacked, though. E.g., attacker putting a VM under your protection or measurement system. DUTCH is an attempt to protect against these threats, and 0-day attacks.

The DUTCH approach is a PCI Express card with an embedded firewall, IDS, and OOB memory analysis. OS and application reference comparison, forensic snapshot, OS and application configuration management. RM ought to be using this. DUTCH was developed as an IRAD; they are looking for someone who wants to use it.

LM Enhanced Security Initiative (ESI): the people responsible for all the recent positive changes in LM's internal security, including stronger passwords, web category blocking, peer-to-peer, and disabling of auto-run on Microsoft Windows.

SOC to SIC transformation: security operations centre (tools, vendor-driven, event-by-event analysis, tools initiate action ('alert'). Security intelligence centre: focus on people and collaboration, threat-driven response, deep understanding of threat, intent, capabilities, countries. LM is offerring this service to CIA.

LM Cyber University: list of top desired skills (secure code development is HOT); top certifications; cyber university training plan. In future, expect programmes to carry the responsibility for training of their own people. Lockheed will provide less instructor-led training opportunities.

References