File 20110725.1600: Notes from meeting with Kevin Miller: all DoD computer systems are required to run Host based Security System (HBSS) now, which is essentially McAfee suite. It contains a HIDS and other goodies, and runs on Windows, Solaris, and other operating systems. Boyd Fletcher has made it known from NSA throughout DoD that guards are not required to run HBSS because it would be too much, and Kevin is writing a paragraph to justify that. Instead, guards will be required to implement SCAP, a protocol to report their patch levels, version numbers, integrity levels, etc. to somewhere. Kevin just got a request from the IAVA people to list all the FOSS running on the guard, a request the developer sees as unreasonable. The developer does not want the world to know just what versions of FOSS are running on the guard, for risk reasons; the DoD are thinking of FOSS as if its standalone utilities running on a Windows machine, so they want to track versions and patches there just like COTS software on Windows machines. But guards are different, more like flight-critical software, I said, where no one but the developer is allowed to touch the configuration. I pointed Kevin at SP 800-53 for a possible source of justification based on the different risk management policy of a cross domain system as opposed to a workstation. UPDATE: I edited Kevin's paragraph with additional justification and he sent it out.

Kevin's final justification paragraph emailed out:

> Patches to a Radiant Mercury (RM) system are provided as a patch bundle from the Radiant Mercury Program office (RMPO). The software and hardware configuration of RM are locked down for security and reliability purposes; each component is carefully selected, configured and maintained. The RMPO makes use of the OCRS IAVA reporting system and responds to applicable advisories. The RMPO monitors FOSS/COTS vendor advisories and other security vulnerability information sources and responds to vulnerabilities that may be discovered. In most cases patches are delivered to each RM deployment through a mail-out CD or DVD patch bundle. Sites cannot apply any patches to the Certified and Accredited PL4 Radiant Mercury system unless directed to do so by the RMPO. The RMPO works with the UCDMO, NSA, DIA and other supporting organizations to ensure that a patch bundle works as expected and does not introduce new issues to the system. When new patch bundles are issued, a formal regression test occurs and depending on the scope of the patch the UCDMO with its supporting agencies may recertify the RM software. In no case is software not tested as part of the approved software baseline able to be installed by sites on their RM systems.

References