From: "Kelvin Nilsen" <kelvin@aonix.com>
Subject: **Breakout summary from 3rd Layered Assurance Workshop**
Date: August 5, 2009 4:47:21 PM PDT
To: "'Rance DeLong'" <rdelong@engr.scu.edu>

Hi Rance,

Here are the bullet points from the 2nd day, 3rd breakout group, addressing the topic "Pragmatic composition of secure software".

1. System analysis to determine certification requirements must precede and guide architecture work.

2. Partition the system architecture to minimize the requirement for certification. In the ideal, the majority of software will be
pushed into realms that require no certification or less stringent certification.

3. System analysts must participate in the selection of COTS components and design of architecture.

3a) Expect feedback from this step, because the choice of COTS components may impact the system architecture and security model.

3b) Choose COTS components that are compatible with certification requirements.

4. COTS vendors should facilitate certification by documenting requirements, traceability, development processes, test plans and
coverage analysis to enable composition of COTS software with other COTS components and with application code.

4a) Most COTS software does not provide this certification evidence. Pragmatic concerns suggest that COTS software that does not
have certification evidence may not be compatible with certification requirements.

4b) For pragmatic reasons, do not "tailor" the COTS components, as this will add significantly to the costs of ongoing
maintenance. COTS vendors should provide configuration options as part of their standard products.