

Panel: MAJOR QUESTIONS IN APPLYING THE SSE-CMM

Panel Chair: Joel E. Sachs, SSE-CMM Steering Group Representative
The Sachs Groups, P.O. Box 6340, Annapolis, MD, 21401
410-269-7714 (voice), 410-956-0604 (fax), sachs@interramp.com (e-mail)

Panelists: Product Evaluator Representative Product Development Representative
System Certification Representative System Integration Representative
Acquisition Representative

A Capability Maturity Model for security engineering called the SSE-CMM is being developed through community-based participation by those involved in integration, development, products, acquisition, evaluation, certification, and accreditation. Government sponsorship is being provided for facilitation, technical support, and promotion. The SSE-CMM should advance security engineering as defined, mature, and measurable discipline to enable:

- a) selection of appropriately qualified providers of security engineering through differentiating bidders by capability levels and by associated programmatic risks;
- b) focused investments in security engineering tools, training, process definition, management practices, and improvements by engineering groups; and
- c) capability-based assurance, i.e., trustworthiness based on confidence in the maturity of an engineering group's security practices and processes.

This panel will explore questions regarding potential major concerns relative to the actual application and use of the SSE CMM. This will be accomplished by comparing points of views from those who supply and those that consume security engineering. Opposing views will be debated so that the issues will be fully understood from key perspectives. Results from SSE-CMM pilots (discussed in the previous forum) as well as extrapolations from the results with other CMMs will be given during the panel.

The panelist will cover the following perspectives relative to being consumers and suppliers of security engineering. These are summarized below:

Security Engineering Consumers
Acquisition Authority
Accreditation Authority
System Certifier
Integrator
Product Evaluator

Security Engineering Suppliers
System Administrator
System Certifier
Integrator
Product Evaluator
Product Vendor

Questions will be examined in three areas. Each question will be addressed by relevant panelists from their perspective as a supplier or consumer relative to the focus of the question. Questions by area include:

Engineering and Improvement

- What are the outputs from security engineering process (when view in terms of a production) for product development, system integration, system administration, and enterprise definition?
- Can integration of security processes into larger effort, e.g. overall system integration, administration, be assumed?
- Can the SSE-CMM aid in establishing security engineering as discipline? defined? mature? measurable?

- Can the SSE-CMM facilitate comparisons of security engineering practices?
- Can the SSE-CMM replace need for produced evidence?

Assurance

- In what ways can a more predictable process contribute to better evidence from the product developer or system integrator?
- In what ways can a more predictable process contribute to better evidence from the product evaluator or system certifier?
- In what ways can a predictable process be relied on as predictor of product or system assurance?
- In what ways can a predictable process be relied on to focus independent product evaluation or system certification?
- In what ways can higher mature levels relate to higher assurance levels?

Supplier Qualification and Selection

- Can the SSE-CMM provide a valid discriminator for security engineering? Can it be the sole discriminator?
- Can self-assessment be appropriate for source selection? Or is independent evaluation necessary? In either can the SSE-CMM expedite source selection?
- Can the SSE-CMM actually guarantee that the security processes are followed?
- Can the SSE-CMM replace the need for specifying security requirements in an acquisition?
- What is the most useful way of reflecting SSE-CMM ratings, e.g. a PA profile, BP profile, or a overall simple level number?