ISO/IEC 21827
Systems Security Engineering Capability Maturity Model (SSE-CMM)

A Process Driven Framework for Assurance
ISSEA is an industry organization that …

- promotes and enhances the Systems Security Engineering –Capability Maturity Model (SSE-CMM / ISO 21827) and derivatives
  - Transportation Sector derivative (published)
  - Medical Sector (Under consideration)
  - Financial Sector (Under consideration)
- dedicated to the advancement of systems security engineering as a defined and measurable discipline
- running an ongoing effort to identify opportunities to collaborate with other initiatives for aligning with SSE CMM to promote mature security capability among system and software developers
Assurance Road Map

- The ISO/IEC 21827 can help...
  - Identify Security Goals
  - Assess Security Posture
  - Support Security Life Cycle
    - Identify Risks
    - Establish Security Requirements
    - Implement Controls
    - Determine Effectiveness
ISO/IEC 21827 is a content-independent standard, which facilitates implementation of a good process for ANY set of security practices.
ISO/IEC 21827
Model Dimensions

DOMAIN
(Process Areas)

CAPABILITY LEVEL
(Common Features)

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimizing
# Model Process Areas

<table>
<thead>
<tr>
<th>Security Engineering Process Areas</th>
<th># of Base Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer Security Controls</td>
<td>4</td>
</tr>
<tr>
<td>Assess Impact</td>
<td>6</td>
</tr>
<tr>
<td>Assess Security Risk</td>
<td>6</td>
</tr>
<tr>
<td>Assess Threat</td>
<td>6</td>
</tr>
<tr>
<td>Assess Vulnerability</td>
<td>5</td>
</tr>
<tr>
<td>Build Assurance Argument</td>
<td>5</td>
</tr>
<tr>
<td>Coordinate Security</td>
<td>4</td>
</tr>
<tr>
<td>Monitor Security Posture</td>
<td>7</td>
</tr>
<tr>
<td>Provide Security Input</td>
<td>6</td>
</tr>
<tr>
<td>Specify Security Needs</td>
<td>7</td>
</tr>
<tr>
<td>Verify and Validate Security</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project and Organizational Process Areas</th>
<th># of Base Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure Quality</td>
<td>8</td>
</tr>
<tr>
<td>Manage Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Manage Project Risk</td>
<td>6</td>
</tr>
<tr>
<td>Monitor and Control Technical Effort</td>
<td>6</td>
</tr>
<tr>
<td>Plan Technical Effort</td>
<td>10</td>
</tr>
<tr>
<td>Define Organization’s Security Engineering Process</td>
<td>4</td>
</tr>
<tr>
<td>Improve Organization’s Security Engineering Process</td>
<td>4</td>
</tr>
<tr>
<td>Manage Product Line Evolution</td>
<td>5</td>
</tr>
<tr>
<td>Manage Systems Engineering Support Environment</td>
<td>7</td>
</tr>
<tr>
<td>Provide Ongoing Skills and Knowledge</td>
<td>8</td>
</tr>
<tr>
<td>Coordinate with Suppliers</td>
<td>5</td>
</tr>
</tbody>
</table>
ISO/IEC 21827 Appraisal

- Evidence based appraisal method
  - Provides “As Is” picture
  - Tailored to the organization
  - Supports business/mission objectives
  - Identifies areas for Improvement
Measuring Assurance

- ISO/IEC 21827 compliant processes can be measured and managed to …
  - Tie security practice performance to business and security goals
  - Quantify compliance with standards
  - Measure effectiveness and efficiency of security implementation
  - Identify data used for measurement

- Measures allow us to…
  - Repeat measurement and provide relevant performance trends over time
  - Identify opportunities for corrective actions and formulate action plans
  - Support security improvement and budget recommendations
  - Produce evidence that substantiates assurance cases
Summary

- ISO/IEC 21827 provides a roadmap for establishing and maturing security practices
  - Process Areas identify a comprehensive set of base (security) practices
  - Capability Levels define maturity

- ISO/IEC 21827 (SSE-CMM) appraisals
  - use process implementation evidence
  - gain insight into maturity and institutionalization of security processes and practices

- Process implementation evidence
  - results from use of the SSE-CMM
  - creates tangible data that can be leveraged in an assurance case
Contact Information

- **Joyce F. Richardson**  
  (301)313-3927  
  joyce.f.richardson@lmco.com

- **Nadya Bartol**  
  703-377-1252  
  bartol_nadya@bah.com

- **Michele Moss**  
  703-377-1254  
  moss_michele@bah.com

- **www.issea.org**
- **www.sse-cmm.org**

REFERENCES:

- “Measuring Capability Based Assurance” – NETSEC JUNE ’04 Proceedings  
  (Nadya Bartol & Joyce Richardson)
- “ISO/IEC 21827” – version 2.0