System Security Engineering: *Whose Job Is It Anyway?*

NDIA SE Symposium – SSE Track #18703

October 24, 2016

Ms Perri Nejib, Fellow, Northrop Grumman
perri.nejib@ngc.com

Dr Dawn Beyer, Fellow, Lockheed Martin
dawn.m.beyer@lmco.com

Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16
Cybersecurity is **EVERYONE’s** Job

**Systems Security Engineering: Whose Job Is It Anyway?**

**ABSTRACT**

This article delivers a look at current and evolving policy, guidance, and standards surrounding security activities in the systems engineering lifecycle. Emphasis is placed on systems security engineering (SSE) and how application of systems engineering concepts and practices in an agile manner (agile systems engineering) throughout the lifecycle is the way to deal with the dynamic and diverse world of cyber threats to a system (Dove 2014). This paper is a follow-on to "Response to Cyber Security Demands for Agility" (Najib-Beyer 2014) published in the International Council on Systems Engineering (INCOSE) INSIGHT in 2014. The focus of this research was bringing attention to cyber security and the importance of other disciplines towards contributing to secure systems. Since that time many of these domains have further developed their own standards, processes, and guidance in the area of cyber security. What we require now is a way to take these domain-focused concepts and integrate them into and across a systems lifecycle. The best way to achieve this is as part of the systems engineering function. Designing and building secure systems requires a seamless integration of security into systems engineering processes and agile methodologies adopted to constantly revisit, reevaluate, and re-design as part of a risk management process. The framework that will be discussed in this paper will focus on taking currently evolving guidance in SSE and breaking that down into products and tools for systems engineers to easily determine the relationship and value between SSE and systems engineering. In addition, quick reference guides will further enhance and enable successful integration of SSE artifacts into systems engineering artifacts. One of the companion pieces needed in the existing SSE documentation is a mapping of work products/artifacts generated during the lifecycle/technical processes and the responsible and contributing parties. Critical to the success of the new guidance, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160, Systems Security Engineering, is a clear accountability and acceptance of all disciplines on their contributions and influence towards developing a secure system. We present an SSE and responsibilities frameworks concepts for consideration. The framework is an implementation tool to be used along with existing guidance in the area of SSE and systems engineering to clearly demonstrate that program protection is not the responsibility of any one person or discipline, it is the responsibility of an entire team of individuals planning, developing, deploying, operating & maintaining (O&O), and retiring a system. SSE is the "glue" that binds all of this together during the systems engineering lifecycle to enhance system security.

Recent paper published in INCOSE Insight Journal, July 2016
Volume 19 / ISSUE 2


**Program Protection and Secure Systems**

**DoD 5000.02**

**DoD 5200.01, Vol. 1-4**

**DoD 5200.39**

**DoD 5200.44**

**DoD 5230.24**

**DoD 8500.01**

**DoD 8510.01**

---

### Technology

- **What**: A capability element that contributes to the warfighters’ technical advantage (CPI)
- **Who Identifies**: System Engineers with CI/Intel and Security SME support
- **ID Process**: CPI Identification
- **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments
- **Countermeasures**: Anti-Tamper, Classification, Exportability Features, Security, etc.
- **Goal**: “Keep secret stuff in” by preventing the compromise and loss of CPI

---

### Components

- **What**: Mission-critical elements and components
- **Who Identifies**: System Engineers, Logisticians
- **ID Process**: Criticality Analysis
- **Threat Assessment**: Defense Intelligence Agency Threat Analysis Center
- **Countermeasures**: SCRM, Cybersecurity, Anti-counterfeits, software assurance, Trusted Foundry, etc.
- **Goal**: “Keep malicious stuff out” by protecting key mission components

---

### Information

- **What**: Information about applications, processes, capabilities and end-items
- **Who Identifies**: All
- **ID Process**: Identification, criticality analysis, and classification guidance
- **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence assessments
- **Countermeasures**: Cybersecurity, Classification, Export Controls, Security, etc.
- **Goal**: “Keep critical information from getting out” by protecting data from our adversaries

---

**Protecting Warfighting Capability Throughout the Lifecycle**

---

**SYSTEM SECURITY ENGINEERING**

---

Program Protection and Secure Systems is executed through SSE (Reed 2015)
INCOSE SSE/SE Roles & Responsibilities Framework - Origins

• Nejib/Beyer paper on agile security July 2014, INCOSE Insight Journal
• Suggested project during INCOSE IS 2014 SSE working group session
• Timely with new SSE guidance and documents coming out from NIST and OSD (SE)
  – New specialty SSE section in upcoming INCOSE SE Handbook v4
• Need an easy reference responsibility framework to map out relationship between SSE/SE
  – Understandable by both SEs and SSEs
Approach

• Research applicable published Standards and Guidance
  – NIST 800-160
  – ISO 15288
  – INCOSE SE Handbook

• Work focused on taking SSE activities, tasks and deliverables/artifacts and developing framework that can be used across domains and clearly defines critical artifact roles and & responsibilities within SSE and SE

• Make it clear to SEs how to integrate SSE products into related SE products and the value in doing so to manage overall program/system design and risk

The systems security engineering discipline provides the security perspective to the systems engineering processes, activities, tasks, products, and artifacts, with emphasis on system security risk management.
Project Goals

• Integrate artifact roles & responsibilities framework into new INCOSE specialty engineering section on SSE – Chapter 10

• Develop framework so that it can easily be adopted into NIST SP 800-160

---

From DoD 5000 Program Protection Plan

Who is responsible for system security engineering?

Describe the linkage between system security engineering and the Systems Engineering Plan.

How will system security design considerations be addressed?
Progress to Date
### Systems Engineering Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Acquisition</td>
<td>• Life Cycle Model Management</td>
<td>• Project Planning</td>
<td>• Business or Mission Analysis</td>
</tr>
<tr>
<td>• Supply</td>
<td>• Infrastructure Management</td>
<td>• Project Planning and Control</td>
<td>• Stakeholder Needs and Requirements Definition</td>
</tr>
<tr>
<td></td>
<td>• Portfolio Management</td>
<td>• Decision Management</td>
<td>• System Requirements Definition</td>
</tr>
<tr>
<td></td>
<td>• Human Resource Management</td>
<td>• Risk Management</td>
<td>• Architecture Definition</td>
</tr>
<tr>
<td></td>
<td>• Quality Management</td>
<td>• Configuration Management</td>
<td>• Design Definition</td>
</tr>
<tr>
<td></td>
<td>• Knowledge Management</td>
<td>• Information Management</td>
<td>• System Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Measurement</td>
<td>• Implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quality Assurance</td>
<td>• Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Transition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Validation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disposal</td>
</tr>
</tbody>
</table>

**Source:** ISO/IEC/IEEE 15288: 2015

---

**INCOSE SE Handbook & NIST SP 800-160 organized by Processes and associated Activities and Tasks**

**Life Cycle Stages**

- Concept
- Development
- Production
- Utilization
- Support
- Retirement

Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16
Security Built into DoD Acquisition Lifecycle

Alignment of RMF and DoD Acquisition System Activities

RMF Step 1 - Categorize system
  Program Acquisition IA Strategy

RMF Step 2 - Select security controls
  Specify system security baselines in JCIDS

RMF Step 3 - Implement security controls
  ISSS/SSS translates security controls to design requirements and integrates into system specifications
  System security specifications in RFP
  Coordinate TEMP and Security Assessment Plan
  Approve system security design at review points

RMF Step 4 - Assess security controls
  Developmental Test & Evaluation (DT&E)

RMF Step 5 - Authorize system (issue ATO)
  Operational Test & Evaluation (OT&E)

RMF Step 6 - Monitor security controls

Cyber security activities integrated across the system acquisition lifecycle (DISA 2014)
NIST 800-160 broken down by ISO 15288:2015/INCOSE SE processes – expressed in security activities and tasks
Realizes the security aspects of all system elements. The resultant system element satisfies the security architectural design requirements and satisfies security requirements, architecture and design.

**ACTIVITIES**
- Prepare for the security aspects of implementation
- Perform the security aspects of implementation
- Manage results of the security aspects of implementation

**INPUTS**
- Security relevant trade space of cost, capability and assurance (h/w, s/w, firmware, services)
- Supplier agreements, legislation and organizational policy
- Security architecture and security design

**OUTCOMES**
- Security aspects of implementation that constrain the requirements, architecture or design are identified
- Security-relevant or security-informed system element is realized
- System elements are securely packaged and stored
- Enabling systems or services needed for the security aspects of implementation are available
- Traceability of the security aspects of the implemented system elements is established

**ROLES**
- SSE (process owner), IA/CS engineer - SE, HW Engr, S/W Engr, Supply Chain/logistics (contributors)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>The security aspects of the implementation strategy are developed.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>The security aspects of implementation that constrain the requirements, architecture, or design are identified.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>A security-relevant or security-informed system element is realized.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>System elements are securely packaged and stored.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>Any enabling systems or services needed for the security aspects of implementation are available.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
<tr>
<td>Traceability of the security aspects of the implemented system elements is established.</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
<td>Implementation Process (IP) (3.1.7)</td>
</tr>
</tbody>
</table>

Initial Mapping done by Ken Kepchar, INCOSE SSE WG Co-Chair

Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Protection Plan/Security Plan</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSE or CS/IA Engr</td>
<td>S/W, H/W, SE, SC</td>
<td>SEMP</td>
</tr>
</tbody>
</table>

**Legend:**
- **O** – Process Outcome
- **I** – Input to Process
- **H/W** – hardware engr
- **S/W** – software engr
- **SE** – system engr
- **SSE** – sys security engr
- **IA/CS** – Info assurance/cybersecurity
- **IT/SA** – IT/sys admin
- **SC** – supply chain/logistics

Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16
<table>
<thead>
<tr>
<th>SSE Task/Artifact</th>
<th>Business or Mission Analysis</th>
<th>Stakeholder Needs &amp; Requirements</th>
<th>System Architecture Definition</th>
<th>Design Definition</th>
<th>System Analysis</th>
<th>Implementation</th>
<th>Integration</th>
<th>Verification</th>
<th>Transition</th>
<th>Validation</th>
<th>Operation</th>
<th>Maintenance</th>
<th>Disposal</th>
<th>Process/Task owner</th>
<th>Supporting Roles</th>
<th>SE Related Artifact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Security Requirements</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mission Requirements</td>
</tr>
<tr>
<td>Security RVTM</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSE or IA/CS Engr</td>
<td>Initial RVTM</td>
</tr>
<tr>
<td>Updated Security RVTM</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Updated RVTM</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System Architecture</td>
</tr>
<tr>
<td>Security Design</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System Design</td>
</tr>
<tr>
<td>Security Analysis</td>
<td>O</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>SSE or IA/CS Engr</td>
<td>SE, H/W, S/W, logistics, SC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System Analysis</td>
<td></td>
</tr>
<tr>
<td>Security Implementation</td>
<td>O</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>SSE or IA/CS Engr</td>
<td>SE, H/W, S/W, logistics, SC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Implementation Report</td>
<td></td>
</tr>
<tr>
<td>Security Integration Report</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Integration Report</td>
</tr>
<tr>
<td>Final SVRTM</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Final VRTM</td>
</tr>
<tr>
<td>Security Transition Report</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Transition Report</td>
</tr>
<tr>
<td>Security Validation Report</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Validated System</td>
</tr>
</tbody>
</table>

Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16
References


Approved For Public Release #16-1910; Unlimited Distribution, Dated 10/3/16