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?

Perri Nejib, perri.nejib@ngc.com; and **Dawn Beyer**, dawn.m.beyer@lmco.com

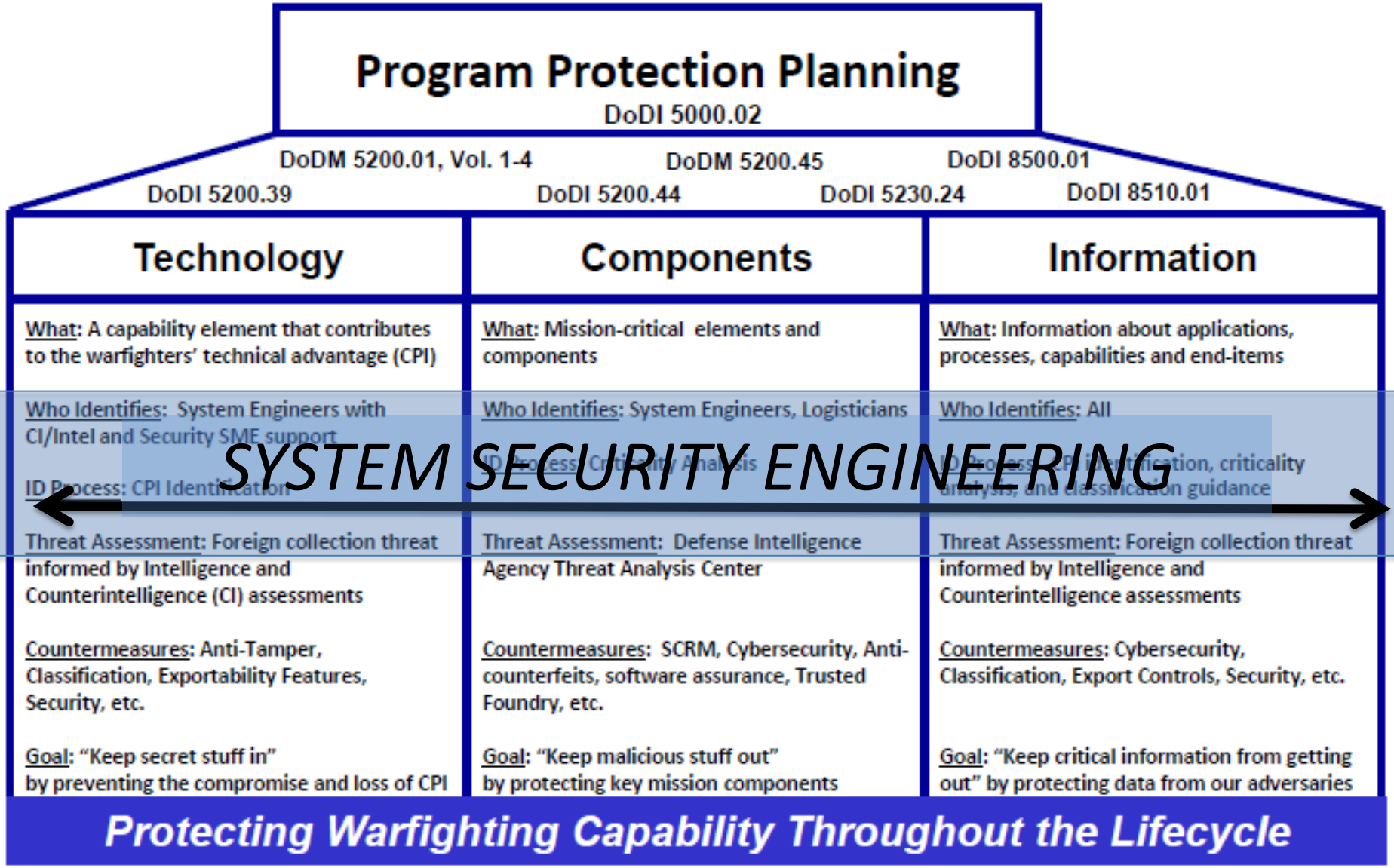
■ **ABSTRACT**

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 processes 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" (Nejib-Beyer 2014) published in the International Council on Systems Engineering (INCOSE) *INSIGHT* in 2014. The focus of that 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 development and 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 roles and responsibilities framework concept 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&M), and retiring a system. SSE is the "glue" that binds all of this together during the systems engineering lifecycle to enhance system security.

Integrating cybersecurity into the SE process is critical to ensuring a secure design

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

Systems Engineering Approach to Cybersecurity is What is Needed



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

These all had major updates mid 2015 and 2016

- 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?

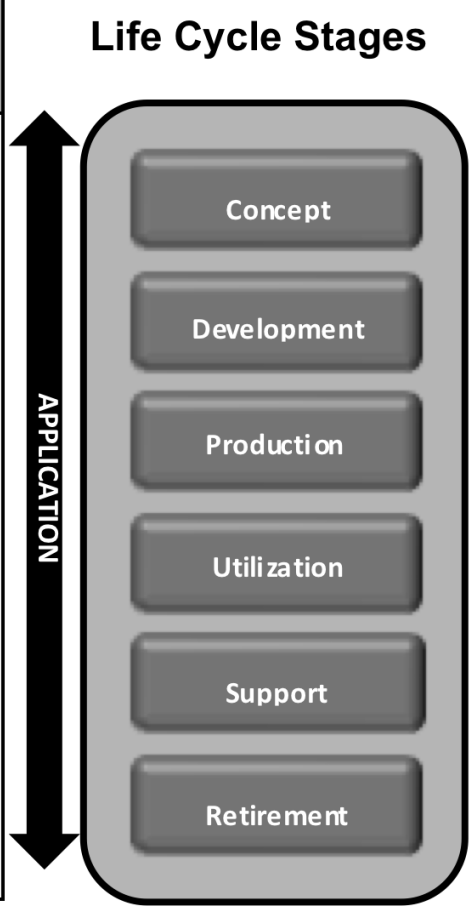
Progress to Date

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

Systems Engineering Life Cycle Processes

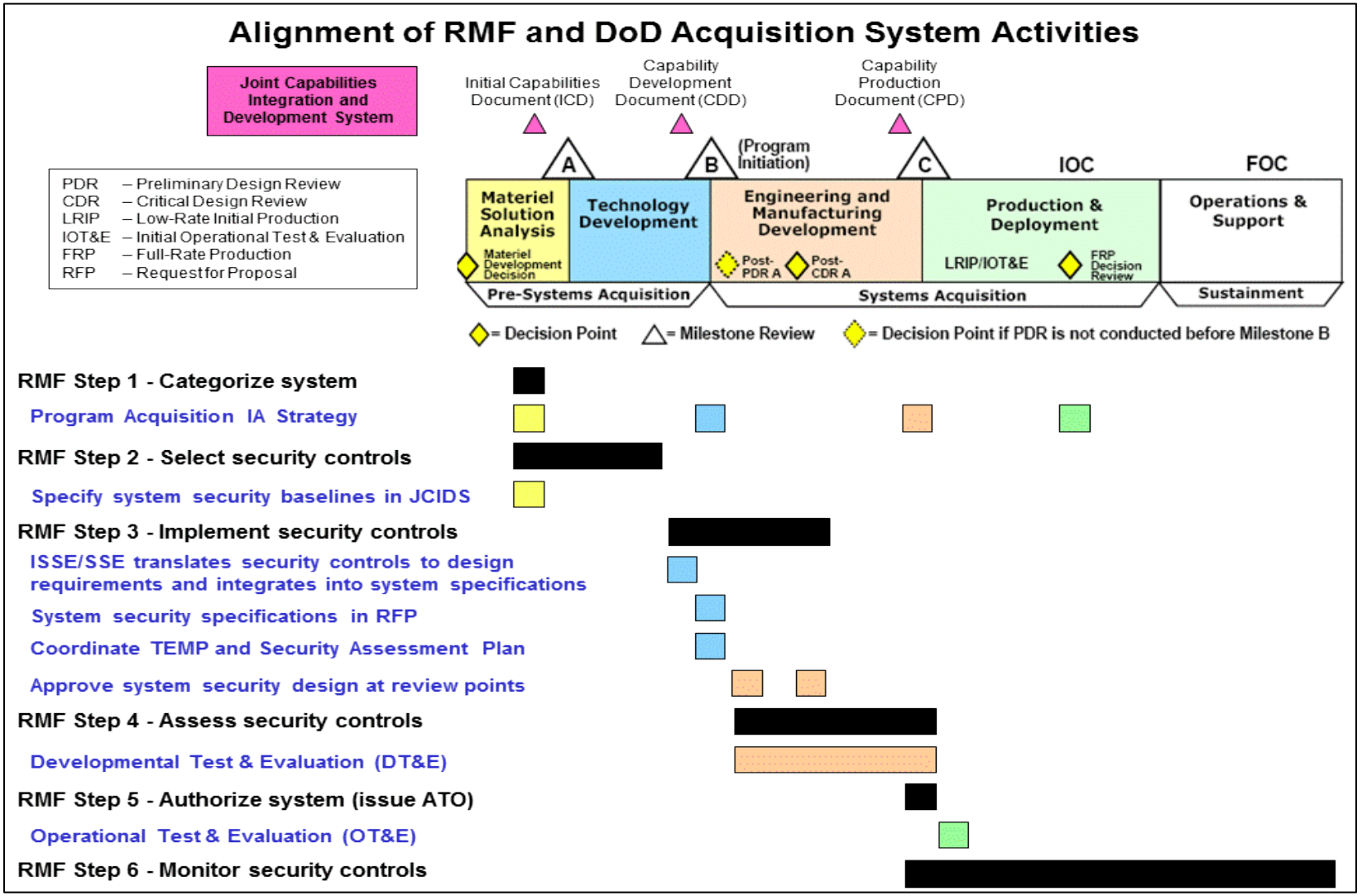
Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal



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

Security Built into DoD Acquisition Lifecycle



Cyber security activities integrated across the system acquisition lifecycle (DISA 2014)

ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

NIST 800-160 broken down by ISO 15288:2015/INCOSE SE processes – expressed in security activities and tasks

IP	Implementation
IP-1	PREPARE FOR THE SECURITY ASPECTS OF IMPLEMENTATION
IP-1.1	Develop the security aspects of the implementation strategy.
IP-1.2	Identify constraints from the security aspects of the implementation strategy and technology on the system requirements, architecture, design, or implementation techniques.
IP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of implementation.

Implementation

Prepare for the security aspects of implementation

Perform…

Manage…

GOAL

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

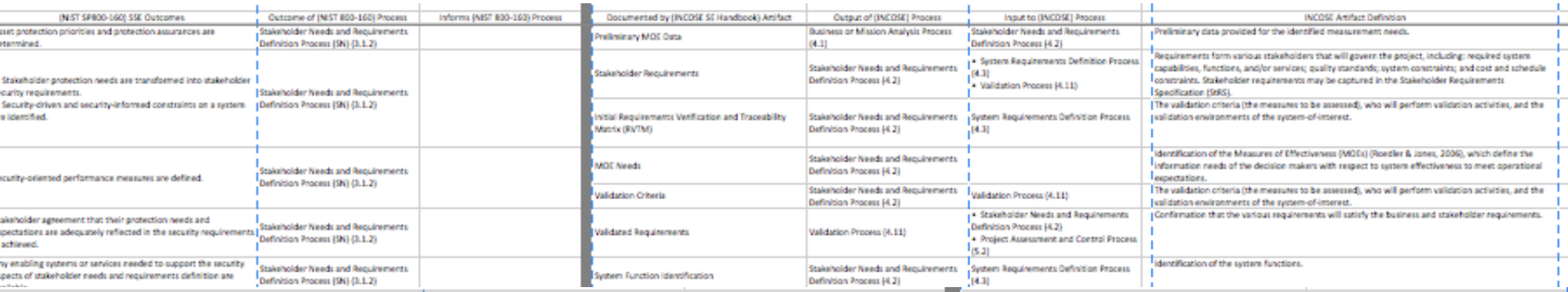
OUTCOMES

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)

NIST 800-160 SSE – ISO/INCOSE SE Mapping



(NIST SP800-160) SSE Outcomes	Outcome of (NIST 800-160) Process	Informs (NIST 800-160) Process	Documented by (INCOSE SE Handbook) Artifact	Output of (INCOSE) Process
	Implementation Process (IP) (3.1.7)			**Implementation Process (4.7)**
The security aspects of the implementation strategy are developed.	Implementation Process (IP) (3.1.7)		Implementation strategy	Implementation Process (4.7)
The security aspects of implementation that constrain the requirements, architecture, or design are identified.	Implementation Process (IP) (3.1.7)		Implementation Constraints	Implementation Process (4.7)
A security-relevant or security-informed system element is realized.	Implementation Process (IP) (3.1.7)		System Elements	Implementation Process (4.7)
			System Element Documentation	Implementation Process (4.7)
System elements are securely packaged and stored.	Implementation Process (IP) (3.1.7)		Implementation Report	Implementation Process (4.7)
Any enabling systems or services needed for the security aspects of implementation are available.	Implementation Process (IP) (3.1.7)		Implementation Enabling System Requirements	Implementation Process (4.7)
Traceability of the security aspects of the implemented system elements is established.	Implementation Process (IP) (3.1.7)		Implementation Traceabilty	Implementation Process (4.7)
			Implementation Record	Implementation Process (4.7)

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

SSE Task/Artifact	Project Planning	Project Assessment and Control	Decision Management	Risk Management	Configuration Management	Information Management	Measurement	Quality Assurance	Process/ Task owner	Supporting Roles	SE Related Artifact
Program Protection Plan/Security Plan	O								SSE or CS/IA Engr	S/W, H/W, SE, SC	SEMP
											Project Performance Measures
											Decision Strategy & Report
Security Risk Management Plan				O					SSE or CS/IA Engr	S/W, H/W, SE, IT/SA	Risk Management Report
											Configuration Management Baselines & Report
											Information Repository
											Measurement Repository
											QA Plan & Report

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

SSE Task/Artifact	Business or Mission Analysis	Stakeholder Needs & Requirements	System Requirements	Architecture Definition	Design Definition	System Analysis	Implementation	Integration	Verification	Transition	Validation	Operation	Maintenance	Disposal	Process/ Task owner	Supporting Roles	SE Related Artifact
Mission Security Requirement	O																Mission Requirements
Security RVTM		O													SSE or IA/CS Engr		Initial RVTM
Updated Security RVTM			O														Updated RVTM
Security Architecture				O													System Architecture
Security Design					O												System Design
Security Analysis						O	I										System Analysis
Security Implementation							O		I		I				SSE or IA/CS Engr	SE, H/W, S/W, logistics, SC	Implementation Report
Security Integration Report								O									Integration Report
Final SVRTM									O								Final VRTM
Security Transition Report										O							Transition Report
Security Validation Report											O						Validated System
Security Operation Report												O					Operation Report
Security maintenance Report													O				Maintenance Report
Security Disposal Report														O			Disposal Report

References

- Slide 3 -Reed, M. 2015. “Systems Security Engineering for Program Protection and Cybersecurity.” Paper presented at the 18th Annual Systems Engineering Conference of NDIA, Springfield, US-VA, 26-29 October. www.dtic.mil/ndia/2015system/18018_Reed.pdf.
- Slides 8,10 – NIST Special Publication 800-160, Systems Security Engineering - *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, pg 22, 25, 27 - Second Public Draft, May 2016*
- Slide 9 - DISA. 2014. Risk Management Framework Implementation. Information Assurance Support Environment. 4 April. http://iase.disa.mil/rmf/Pages/rmf-training.aspx.
- Slide 12 – Kepchar, K. 2016. Mapping of NIST 800-160 processes vs INCOSE Handbook SE Processes, INCOSE SSE Working Group review of NIST 800-160