SEAM

Assurance On Demand™

Secure Engineering Assurance Model

INCOSE
International Council on Systems Engineering

An implementation of Security Engineering
June 11, 2014
INCOSE ABQ Chapter

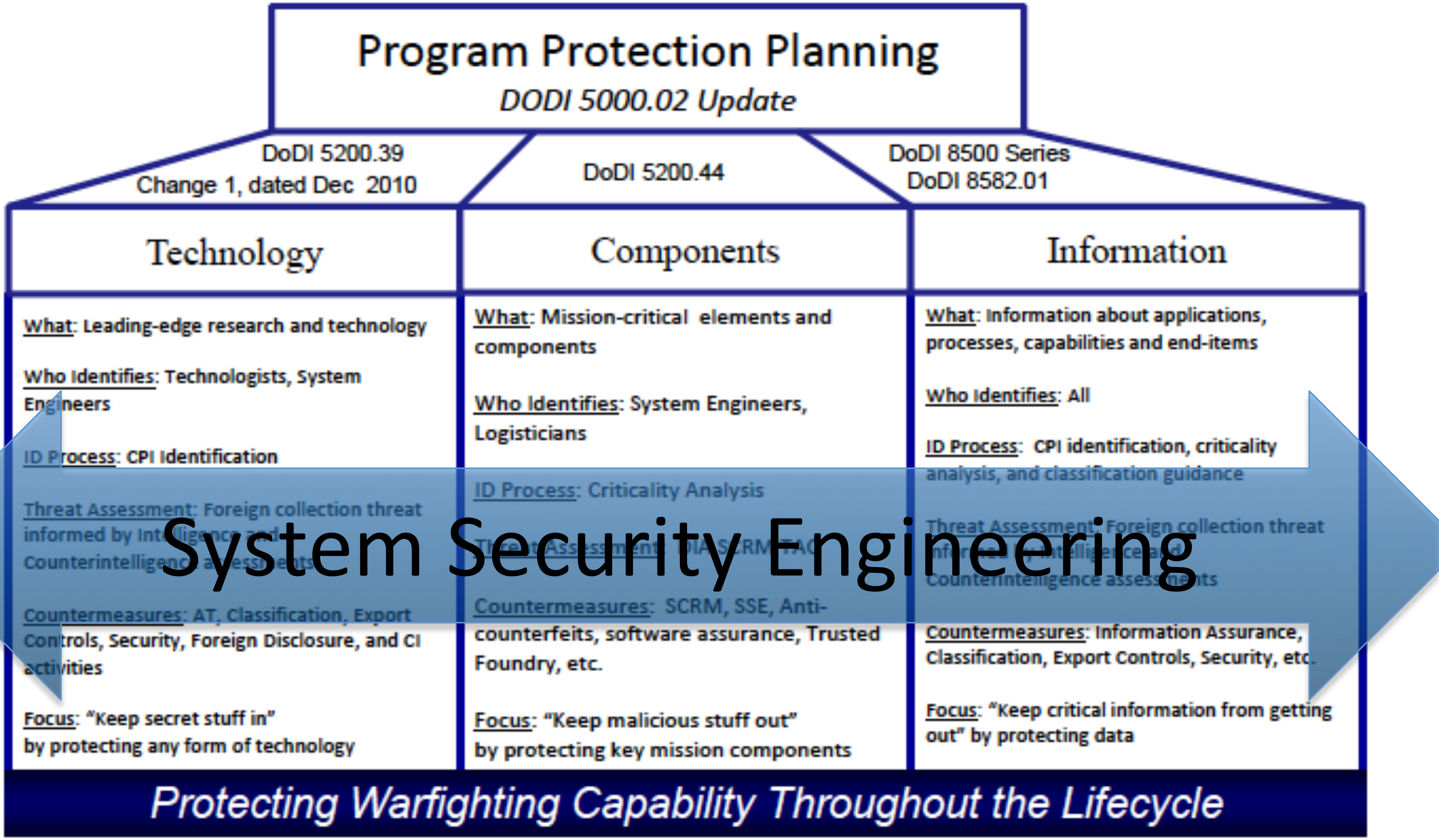
Perri Nejib, Sr. Fellow, CISSP, CIPM, ESEP
Cyber Security Fact Chair
Security Engineering CoP Lead

Dawn Beyer, Fellow, CISSP, PMP, CSSLP, CISM
Security Engineering Domain Advocate
Security Engineering CoP Lead

Agenda

- Why SEAM™?
- Security Challenges
- Security as an Enterprise Concern
- Security Engineering LM Timeline
- Security Engineering Foundations
- Security Engineering Procedure
- Security Engineering Lifecycle
- SEAM™ Concept
- SEAM™ “products”
- Community of Practice/Collaboration
- SEAM™ “Playbook” demo

What Are We Protecting?



Program Protection Planning

DODI 5000.02 Update

DoDI 5200.39
Change 1, dated Dec 2010

DoDI 5200.44

DoDI 8500 Series
DoDI 8582.01

Technology

What: Leading-edge research and technology

Who Identifies: Technologists, System Engineers

ID Process: CPI Identification

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities

Focus: "Keep secret stuff in" by protecting any form of technology

Components

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality Analysis

Threat Assessment: DIA SCRM TAC

Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.

Focus: "Keep malicious stuff out" by protecting key mission components

Information

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.

Focus: "Keep critical information from getting out" by protecting data

System Security Engineering

Protecting Warfighting Capability Throughout the Lifecycle

Distribution Statement A – Approved for public release by OSD on 10/28/2013, SR Case # 14-S-0136 applies. Distribution is unlimited.

SSE Priorities

- **Policy Initiatives**
  - DoDI 5000.02 Operation of the Defense Acquisition System
  - DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD
  - DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
  - DoDI 8500.01E Information Assurance
- **Depth of PPP Analysis throughout the Life Cycle**
- **Protection of Integrated Circuits**
- **Software Assurance**
- **Protection of Defense Industrial Base Systems**
- **Incorporating SSE into Contracts**
- **Program Protection Guidance**
- **Integrated SSE**

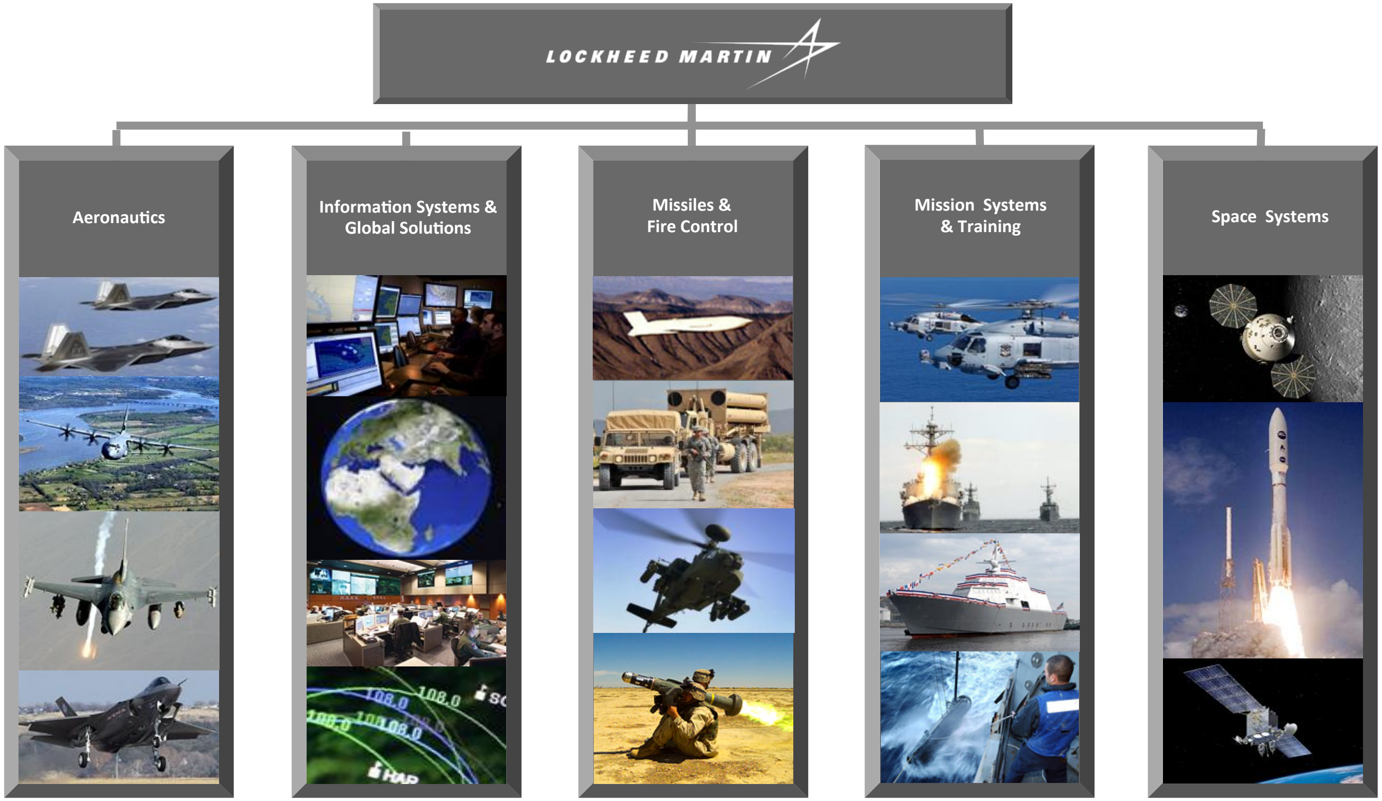
DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle

Distribution Statement A – Approved for public release by OSR on 10/28/2013, SR Case # 14-S-0136 applies. Distribution is unlimited.

Why SSE/SEAM™? Our customers demand secure solutions

LOCKHEED MARTIN

Our main areas of focus are in defense, space, intelligence, homeland security, and information technology, including cyber security



LOCKHEED MARTIN

Aeronautics

Information Systems & Global Solutions

Missiles & Fire Control

Mission Systems & Training

Space Systems

We Never Forgot Who We Are Working For… And Neither Do Our Adversaries

Mission Statement

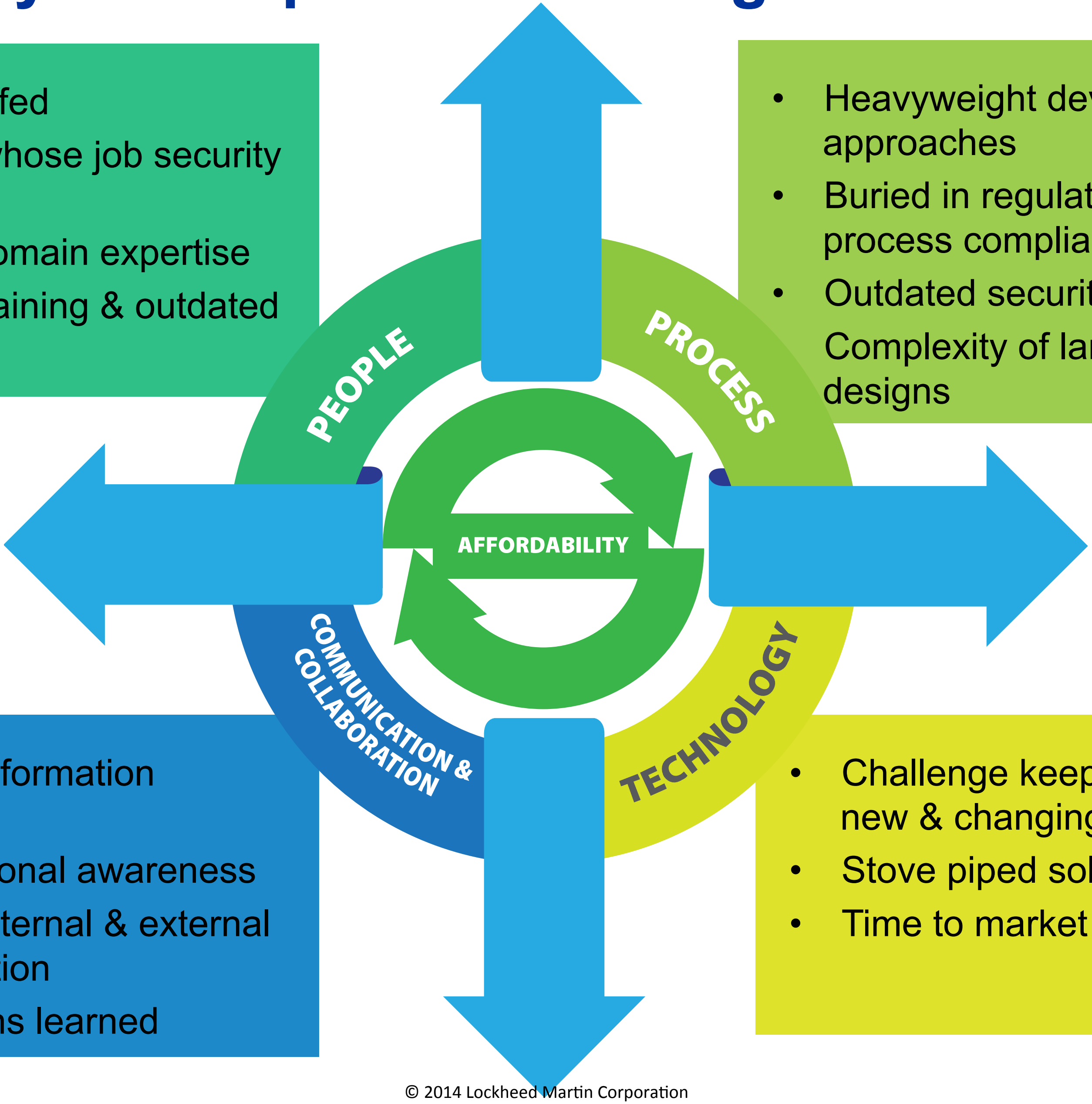
- Integrating Security into Every Solution We Deliver
  - Reducing Risk and Providing Fully Reliable and Trusted Solutions
- Utilizing Best Practices and Rigorous Processes
  - LM Employs a System Security Engineering Process that employs, Cyber security/IA, Anti-Tamper and Secure Supply Chain

Integrated. Proactive. Resilient.

Security Development Challenges

- Understaffed
- Unclear whose job security is
- Lack of domain expertise
- Lack of training & outdated training

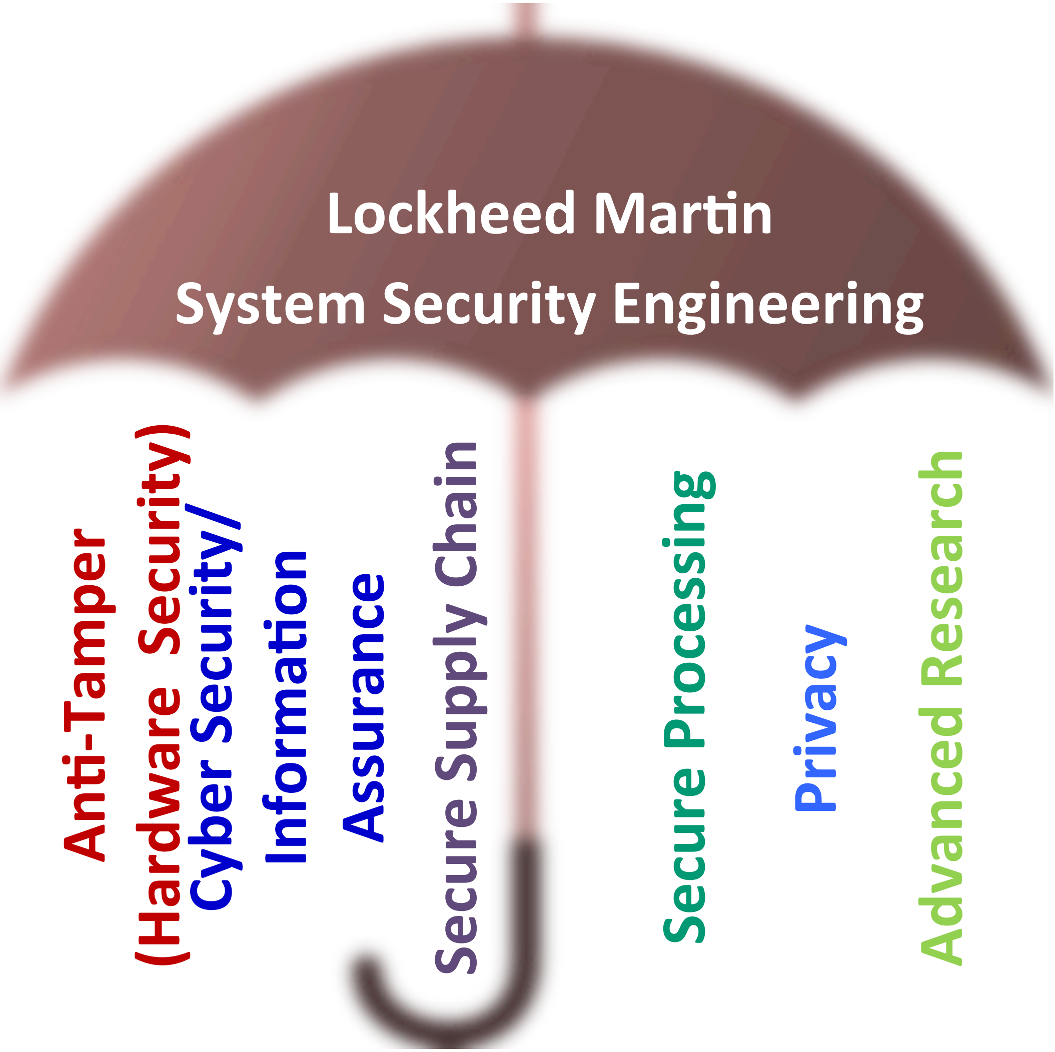
- Heavyweight development approaches
- Buried in regulations & process compliance
- Outdated security practices
- Complexity of large system designs



- Lack of information sharing
- No situational awareness
- Lack of internal & external collaboration
- No lessons learned

- Challenge keeping up with new & changing technology
- Stove piped solutions
- Time to market

Security is an Enterprise-Wide Concern



Lockheed Martin

System Security Engineering

Anti-Tamper (Hardware Security)

Cyber Security/ Information Assurance

Secure Supply Chain

Secure Processing

Privacy

Advanced Research

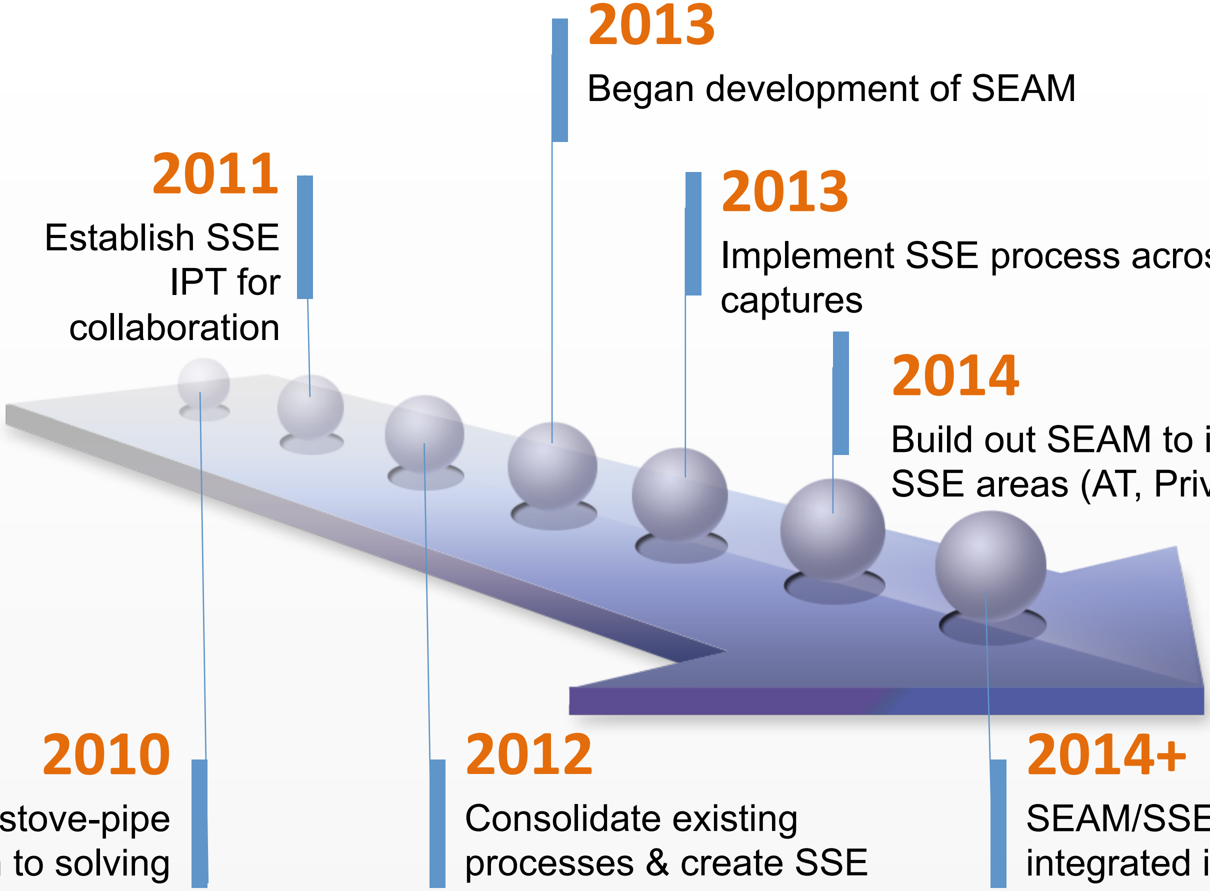
Systems security engineering is comprised of the following sub disciplines:

- Operations Security
- Information Security
- Network Security
- Physical Security
- Personnel Security
- Administrative Security
- Communications Security
- Emanation Security
- Computer Security

ISO/IEC 21827

LM has developed a strong, multi-disciplinary approach

LM SSE Timeline



2010
Reduce stove-pipe approach to solving System Security

2011
Establish SSE IPT for collaboration

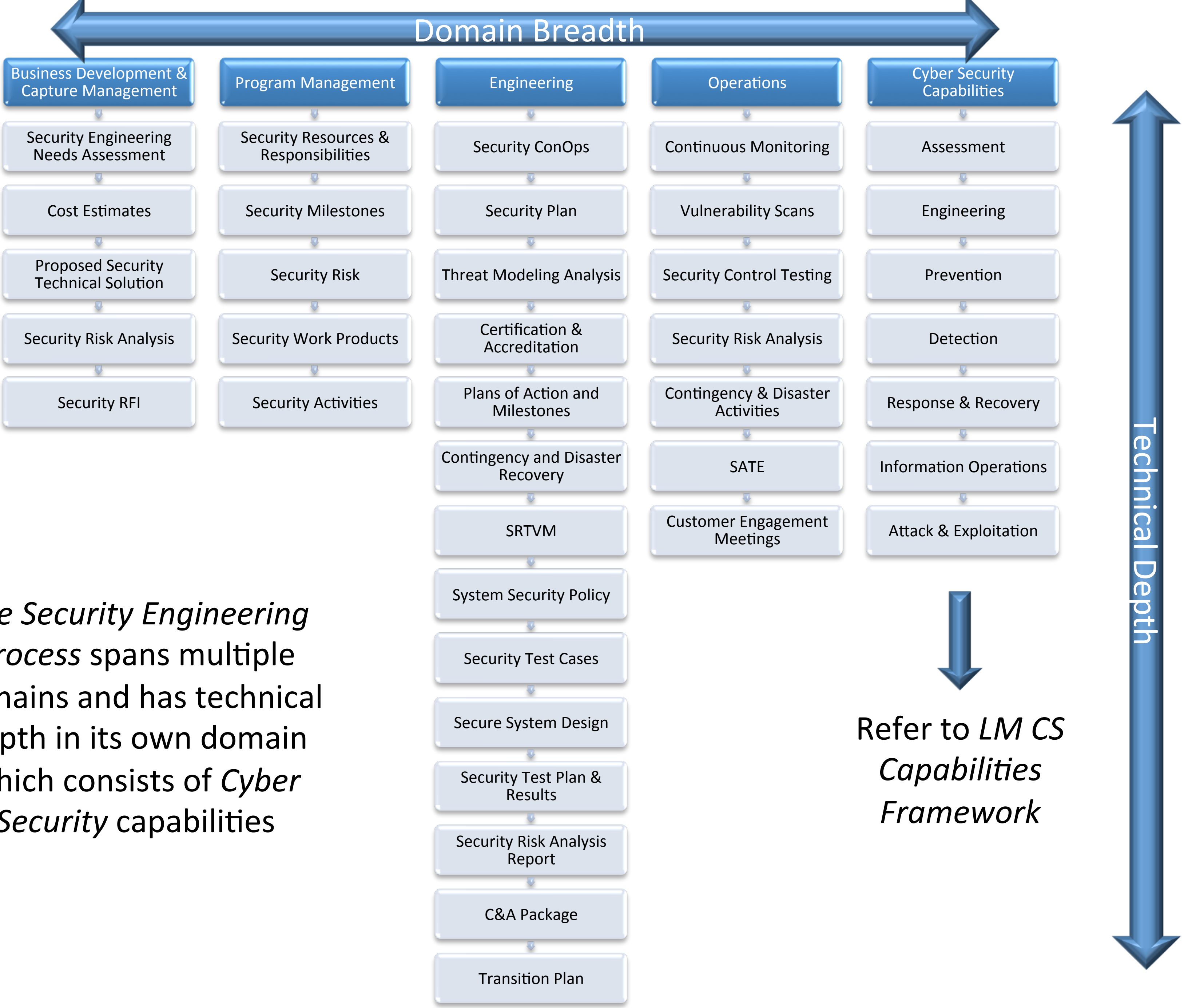
2012
Consolidate existing processes & create SSE Process for all lines of business

2013
Began development of SEAM

2013
Implement SSE process across programs & captures

2014
Build out SEAM to include other SSE areas (AT, Privacy etc.)

2014+
SEAM/SSE fully integrated into systems engineering life cycle



Business Development & Capture Management	Program Management	Engineering	Operations	Cyber Security Capabilities
Security Engineering Needs Assessment	Security Resources & Responsibilities	Security ConOps	Continuous Monitoring	Assessment
Cost Estimates	Security Milestones	Security Plan	Vulnerability Scans	Engineering
Proposed Security Technical Solution	Security Risk	Threat Modeling Analysis	Security Control Testing	Prevention
Security Risk Analysis	Security Work Products	Certification & Accreditation	Security Risk Analysis	Detection
Security RFI	Security Activities	Plans of Action and Milestones	Contingency & Disaster Activities	Response & Recovery
		Contingency and Disaster Recovery	SATE	Information Operations
		SRTVM	Customer Engagement Meetings	Attack & Exploitation
		System Security Policy		
		Security Test Cases		
		Secure System Design		
		Security Test Plan & Results		
		Security Risk Analysis Report		
		C&A Package		
		Transition Plan		

The Security Engineering Process spans multiple domains and has technical depth in its own domain which consists of *Cyber Security* capabilities

Refer to *LM CS Capabilities Framework*

LM Cyber Security Capabilities Framework

Functions/Activities

Assessment	Engineering	Prevention	Detection	Response & Recovery	Information Operations	Attack & Exploitation
Analytical Techs for Security Across IT Sys Eng Life Cycle	Security Engineering Planning	Information Flow Control	Trend Analysis, Mining, Attack Prediction	Business & Operations Continuity Mgmt	Attack & Collection Tools	Control & Concealment
Critical Infrastructure Dependencies & Interdependencies	Security Requirements Engineering	Trusted Computing Base	Performance Monitoring	Incident Handling	Reverse Engineering	Supply Chain Attack
Threat Modeling	Secure Architecture Development	Security Policy Management & Enforcement	Intrusion Detection	Incident Mitigation	Reconnaissance	Insider Attack
Risk-Based Decision Making & Assessments	Secure System Design	Network Security	Malware Detection	Forensics	Counter-Intelligence	Close Attack
New Technology & Product Evaluation	Secure Component & Code Design	Multi-Level Security	Tamper Detection	Reverse Malware Engineering	Situational Awareness & Visualization	Remote Attack
Software Quality Assess, Test, Fault Characterization	HW & SW Anti-Tamper Design	Identity, Access Management	Intrusion Validation & Threat Characterization	Patch Management	Security Information Management	Disruption, Denial, Destruction
SW Integrity & Reverse Engineering	Security Testing, Remediation & Certification	Encryption/ Cryptography	Detection of Hidden Data Flows	Incident Investigation	Cyber Battlefield Management	Data Discovery & Capture
Certification & Accreditation	Security Engineering Management	Content Control	Discovery		Cyber Intelligence	Data Hiding & Exfiltration
Security Value Metrics	Accreditation & Secure System Deployment	Malware Prevention	Supply Chain Security		Deception	Purge & Evacuation
Compliance	Secure System Retirement	Network Protection	Audit & Accountability		Attribution	Cyber Munitions
Security Policy Development & Advocacy		Key Management				Distribution & Delivery
		Physical Security				
		Database Security Administration				
		Security & Awareness Education & Training				
		Privacy				

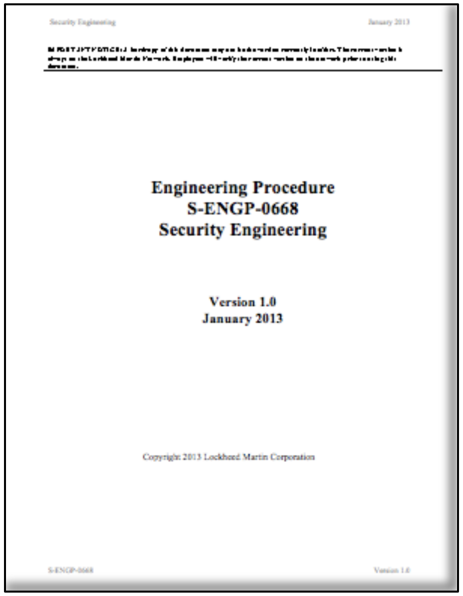
Capabilities

Capabilities broken down into people/ SMEs, processes, best practices, technology

Security Engineering Procedure

LOCKHEED MARTIN

LM has implemented a Security Engineering Procedure for use across all lines of business



Security Engineering January 2013

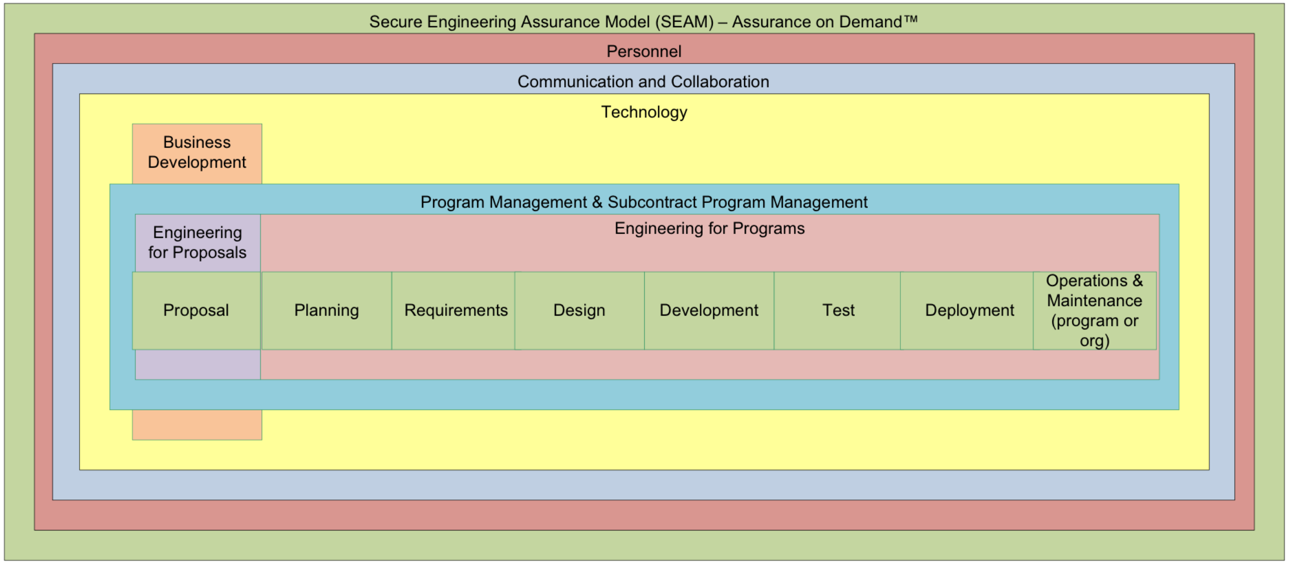
[illegible]

Engineering Procedure
S-ENGP-0668
Security Engineering

Version 1.0
January 2013

Copyright 2013 Lockheed Martin Corporation

S-ENGP-0668 Version 1.0



Secure Engineering Assurance Model (SEAM) – Assurance on Demand™

Personnel

Communication and Collaboration

Technology

Business Development

Program Management & Subcontract Program Management

Engineering for Proposals

Engineering for Programs

Proposal

Planning

Requirements

Design

Development

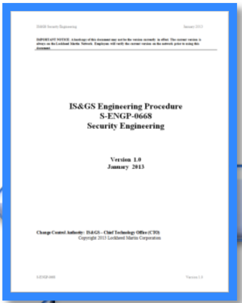
Test

Deployment

Operations & Maintenance (program or org)

- Identifies the security engineering activities, milestones, and work products performed and created throughout the engineering lifecycle from concept to retirement
- Illustrates how security engineering work products integrate into systems engineering deliverables throughout the engineering lifecycle

Security Engineering throughout the Life Cycle



IS&GS Security Engineering January 2013

IMPORTANT NOTICE: A hardcopy of this document may not be the version currently in effect. The current version is always on the Lockheed Martin Network. Employees will verify the current version on the network prior to using this document.

IS&GS Engineering Procedure
S-ENGP-0668
Security Engineering

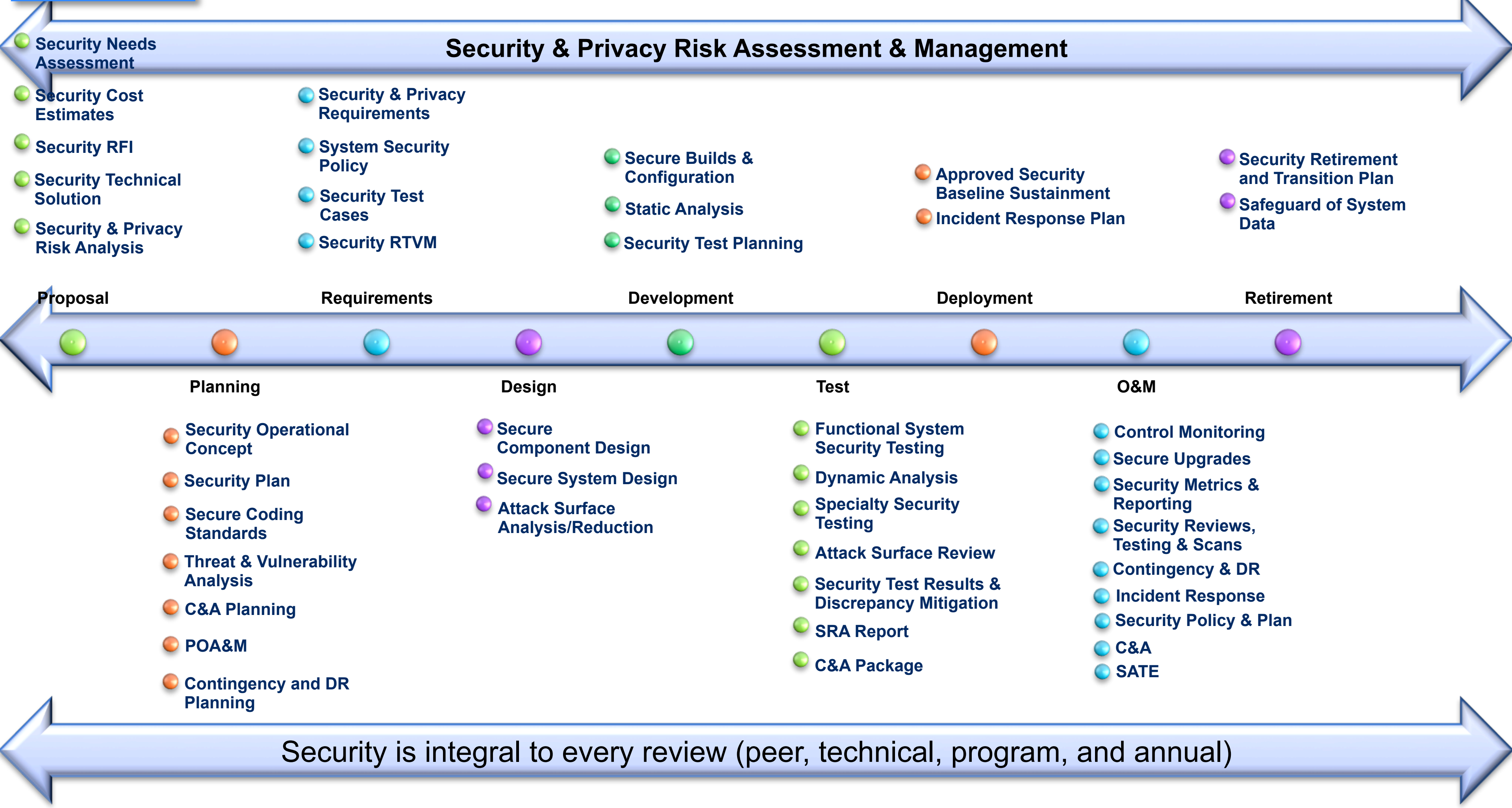
Version 1.0
January 2013

Change Control Authority: IS&GS – Chief Technology Office (CTO)
Copyright 2013 Lockheed Martin Corporation

S-ENGP-0668 Version 1.0

Continuous Improvement

Lean - Agile - Lessons Learned - Best Practices - Process/Procedure Maturity - Metrics Collection & Analysis



Security & Privacy Risk Assessment & Management

Proposal

- Security Needs Assessment
- Security Cost Estimates
- Security RFI
- Security Technical Solution
- Security & Privacy Risk Analysis

Planning

- Security Operational Concept
- Security Plan
- Secure Coding Standards
- Threat & Vulnerability Analysis
- C&A Planning
- POA&M
- Contingency and DR Planning

Requirements

- Security & Privacy Requirements
- System Security Policy
- Security Test Cases
- Security RTVM

Design

- Secure Component Design
- Secure System Design
- Attack Surface Analysis/Reduction

Development

- Secure Builds & Configuration
- Static Analysis
- Security Test Planning

Test

- Functional System Security Testing
- Dynamic Analysis
- Specialty Security Testing
- Attack Surface Review
- Security Test Results & Discrepancy Mitigation
- SRA Report
- C&A Package

Deployment

- Approved Security Baseline Sustainment
- Incident Response Plan

O&M

- Control Monitoring
- Secure Upgrades
- Security Metrics & Reporting
- Security Reviews, Testing & Scans
- Contingency & DR
- Incident Response
- Security Policy & Plan
- C&A
- SATE

Retirement

- Security Retirement and Transition Plan
- Safeguard of System Data

Security is integral to every review (peer, technical, program, and annual)

Note: this is a framework which should be tailored to a methodology

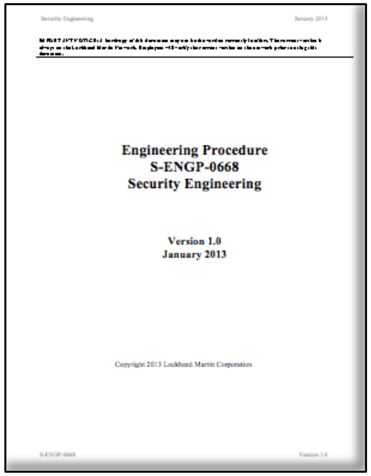
Refer to IS&GS S-ENGP-0668

Integration of SSE process into other domain's processes for success

LOCKHEED MARTIN

COMMAND MEDIA CENTRAL
for Lockheed Martin policies, processes, and procedures

IS&GS PROCESS STORE



Security Engineering January 2013

Engineering Procedure
S-ENGP-0668
Security Engineering

Version 1.0
January 2013

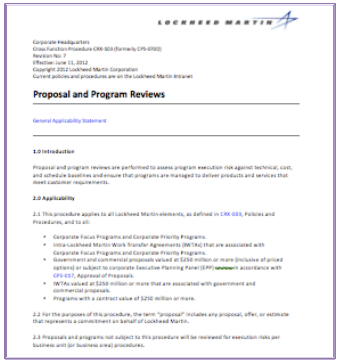
Copyright 2013 Lockheed Martin Corporation

S-ENGP-0668 Version 1.0

SSE Process
S-ENGP-0668

Business Development / Capture Process

RS-BDEV-0009



LOCKHEED MARTIN

Corporate Headquarters
Cross Function Procedure CRX-103 (formerly CPS-0700)
Revision No: 7
Effective: June 11, 2012
Copyright 2012 Lockheed Martin Corporation
Current policies and procedures are on the Lockheed Martin Intranet

Proposal and Program Reviews

General Applicability Statement

1.0 Introduction

Proposal and program reviews are performed to assess program execution risk against technical, cost, and schedule baselines and ensure that programs are managed to deliver products and services that meet customer requirements.

2.0 Applicability

2.1 This procedure applies to all Lockheed Martin elements, as defined in CRX-003, Policies and Procedures, and to all:

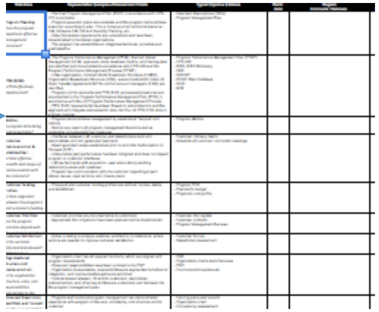
- Corporate Focus Programs and Corporate Priority Programs.
- Intra-Lockheed Martin Work Transfer Agreements (IWTAs) that are associated with Corporate Focus Programs and Corporate Priority Programs.
- Government and commercial proposals valued at $250 million or more (inclusive of priced options) or subject to corporate Executive Planning Panel (EPP) ~~review~~ in accordance with CPS-017, Approval of Proposals.
- IWTAs valued at $250 million or more that are associated with government and commercial proposals.
- Programs with a contract value of $250 million or more.

2.2 For the purposes of this procedure, the term "proposal" includes any proposal, offer, or estimate that represents a commitment on behalf of Lockheed Martin.

2.3 Proposals and programs not subject to this procedure will be reviewed for execution risks per business unit (or business area) procedures.

Program Management

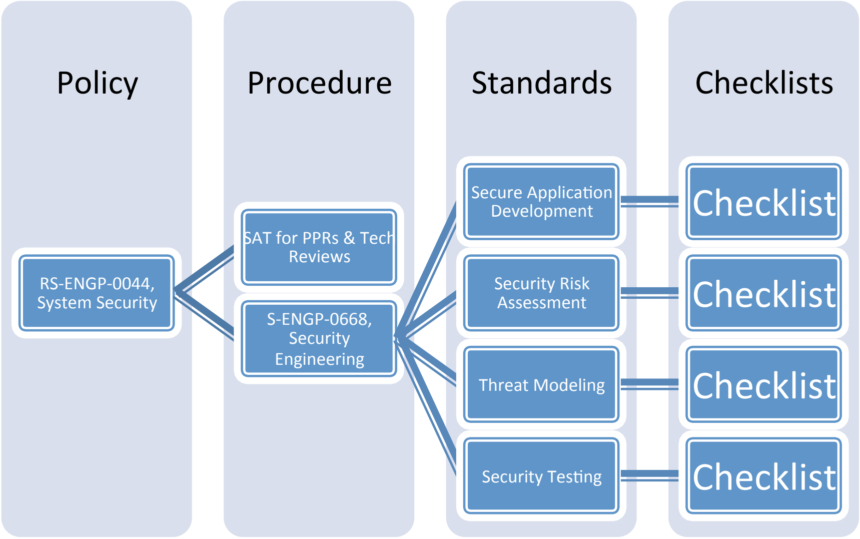
Process PM-001-1



Proposal/Program Review Process (PPRP) representatives – Risk Review Board

A model created to "SEAM" together people, process and tools across a system life cycle/ organization to reduce cyber security risk to system/program

- Security Engineering best practices, processes, standards, and checklists/tools
- Integrates security throughout a systems life cycle
- Develops a culture of security responsibility within all program and engineering disciplines
- Rooted in community- and corporate-recognized standards and industry best practices
- Agile and constantly evolving process to respond to dynamic cyber-threat environment
- Constant feedback loop where operations provides information back into development as new threats are identified



Policy

Procedure

Standards

Checklists

RS-ENGP-0044, System Security

SAT for PPRs & Tech Reviews

S-ENGP-0668, Security Engineering

Secure Application Development

Security Risk Assessment

Threat Modeling

Security Testing

Checklist

Checklist

Checklist

Checklist

▪**SEAM™ breaks down the Security Engineering policy & procedure into standards and checklists applicable to all program staff (eg. Business development, Program managers, Capture managers, software developers, system engineers)**

SEAM Assurance On Demand™

Secure Engineering Assurance Model

Info-assurance eForum (459 Subscribers)

Storefront

SECURITY ENGINEERING

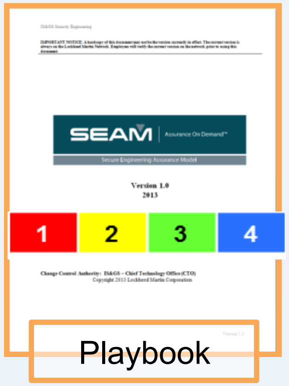
Join Our eForum!

JOIN NOW

Talent Finder

LM Security Engineering DA IPT

Communication & Collaboration



IS&GS Security Engineering

IMPORTANT NOTICE: A hardcopy of this document may not be the version currently in effect. The current version is always on the Lockheed Martin Network. Employees will verify the current version on the network prior to using this document.

SEAM Assurance On Demand™

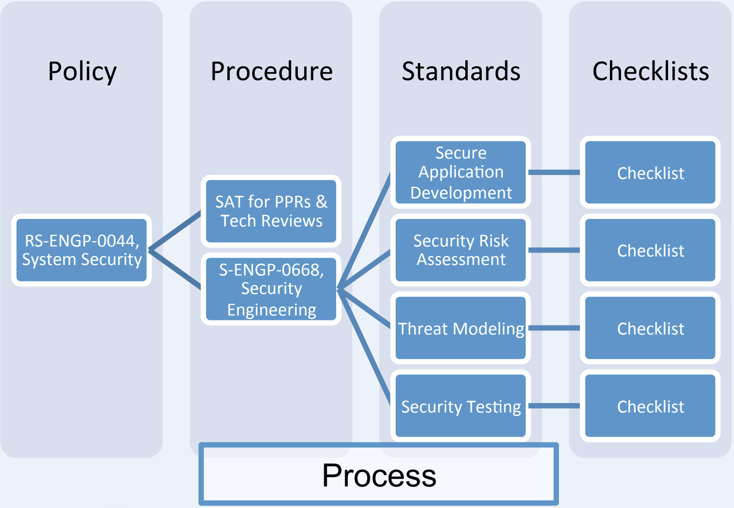
Secure Engineering Assurance Model

Version 1.0
2013

1 2 3 4

Change Control Authority: IS&GS – Chief Technology Office (CTO)
Copyright 2013 Lockheed Martin Corporation

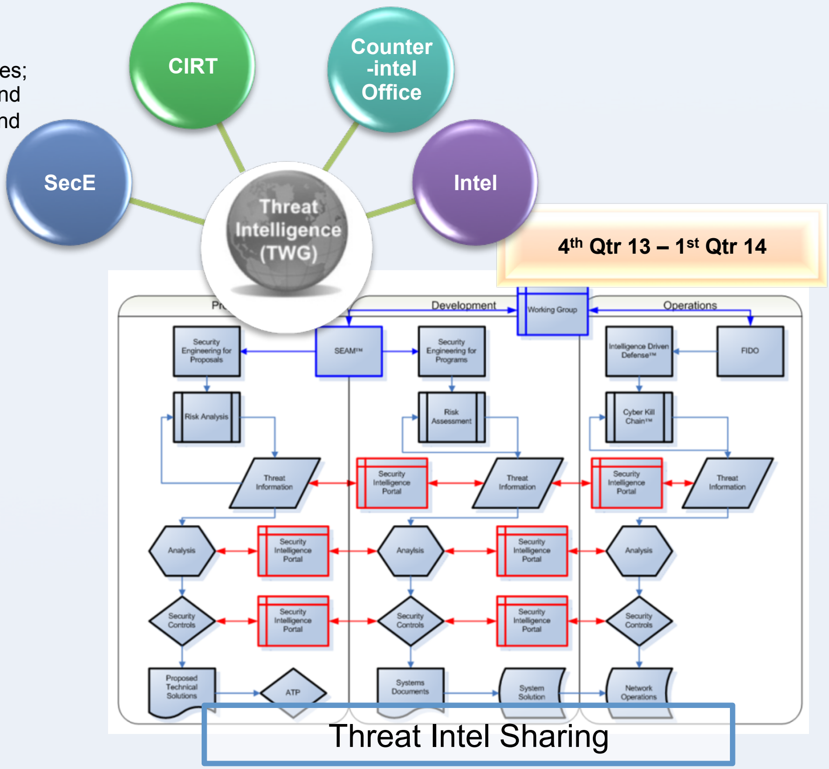
Playbook



Policy	Procedure	Standards	Checklists
RS-ENGP-0044, System Security	SAT for PPRs & Tech Reviews	Secure Application Development	Checklist
	S-ENGP-0668, Security Engineering	Security Risk Assessment	Checklist
		Threat Modeling	Checklist
		Security Testing	Checklist

Process

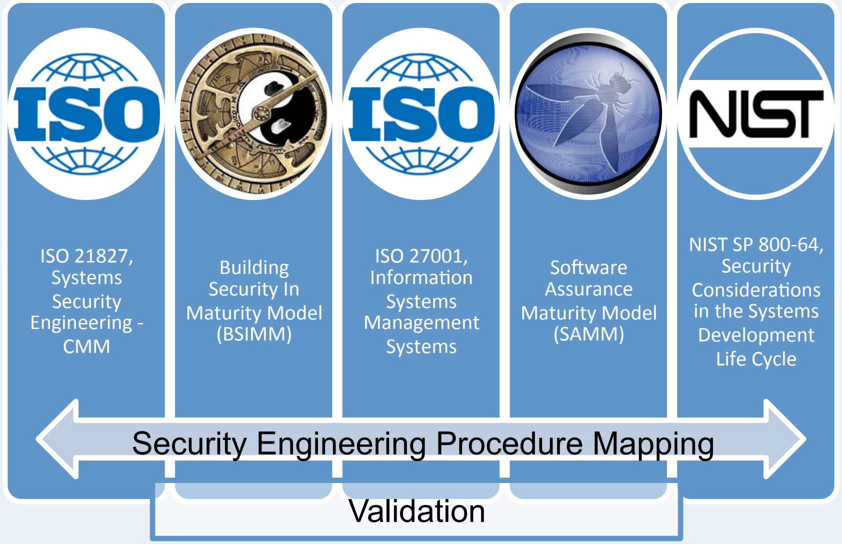
SEAM™ Solution
On-Demand
Agile
Tailorable
Measures Risk
Contains: Checklists & Best Practices; Assessments & Maturity Ratings; and Reference to People, Processes, and Technology



CIRT
Counter -intel Office
SecE
Intel
Threat Intelligence (TWG)
Pr
Development
Working Group
Operations
Security Engineering for Proposals
SEAM™
Security Engineering for Programs
Intelligence Driven Defense™
FIDO
Risk Analysis
Risk Assessment
Cyber Kill Chain™
Threat Information
Security Intelligence Portal
Threat Information
Security Intelligence Portal
Threat Information
Analysis
Security Intelligence Portal
Anaylsis
Security Intelligence Portal
Analysis
Security Controls
Security Intelligence Portal
Security Controls
Security Intelligence Portal
Security Controls
Proposed Technical Solutions
ATP
Systems Documents
System Solution
Network Operations

4th Qtr 13 – 1st Qtr 14

Threat Intel Sharing



ISO 21827, Systems Security Engineering - CMM

Building Security In Maturity Model (BSIMM)

ISO 27001, Information Systems Management Systems

Software Assurance Maturity Model (SAMM)

NIST SP 800-64, Security Considerations in the Systems Development Life Cycle

Security Engineering Procedure Mapping

Validation

Developed under SEAM™ to assist in the Capture/Proposal/Program management portions of the lifecycle

Cyber Security

References

Purpose of Federal Information Security – To ensure the availability, integrity and confidentiality (CIA) of federal information/data, info systems and IT

DODI 5000.2 Defense Acquisition Guidebook – IA Section

"Programs that have IT have IA"
"Programs deemed Mission Critical or Mission Essential requires IA Strategy"
"IT that is connected to the GIG"

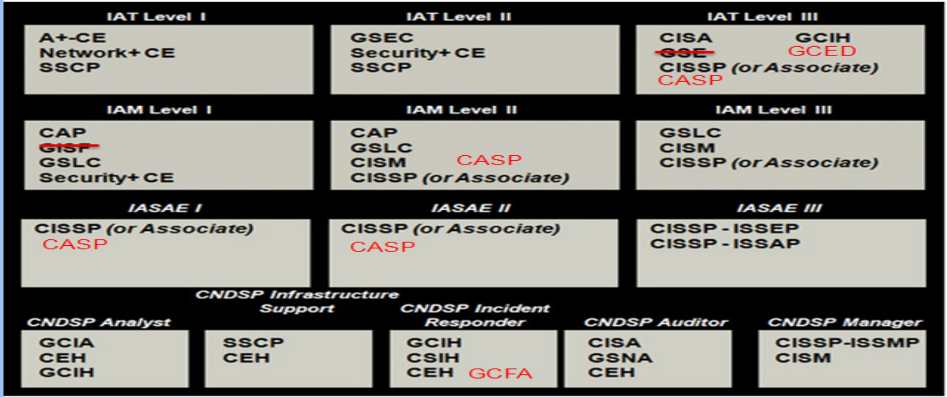
OMB Circular A-130 Appendix III – Security of Federal Automated Information Systems (AIS) describes:

- Minimum set of controls linked to OMB Circular A-123
- Assigns security responsibility

8500 Series

DODD 8500.1 – Overarching policy on IA
DODI 8500.2 – IA controls and implementation
DODI 8510.01 – RMF for DoD IT
ICD 503 – IC policy for IT system security risk management, C&A
ICD 502 – Integrated defense of the information environment for the IC
DIARMF/NIST SP 800-37 – Risk framework assessment and authorization

Critical Infrastructure (financial, energy, water, pharma) – NIST



IAT Level I	IAT Level II	IAT Level III
A+-CE Network+ CE SSCP	GSEC Security+ CE SSCP	CISA ~~GSE~~ CISSP *(or Associate)* CASP GCIH GCED
IAM Level I	**IAM Level II**	**IAM Level III**
CAP ~~GISP~~ GSLC Security+ CE	CAP GSLC CISM CISSP *(or Associate)* CASP	GSLC CISM CISSP *(or Associate)*
IASAE I	***IASAE II***	***IASAE III***
CISSP *(or Associate)* CASP	CISSP *(or Associate)* CASP	CISSP - ISSEP CISSP - ISSAP

CNDSP Analyst	*CNDSP Infrastructure Support*	*CNDSP Incident Responder*	*CNDSP Auditor*	*CNDSP Manager*
GCIA CEH GCIH	SSCP CEH	GCIH CSIH CEH GCFA	CISA GSNA CEH	CISSP-ISSMP CISM

Security-related staff certifications per ISO 17024/DoDM 8570.1 IA training, certification and workforce management

system that support the operations and assets of the agency – Title III of the E-Government Act of 2002

FIPS series – Federal Information Processing Standards series relating to standards and guidelines adopted under the provisions of the FISMA: FIPS 140-2 Security reqmts for crypto modules
FIPS -199 Standards for security categorization of info sys
FIPS 200 Minimum security reqmts for info sys

Special Publication (SP) 800-series

SP 800-30 Risk Mngmt Guide for IT
SP 800-37 Guidelines for C&A of IT
SP 800-53 Recommended security controls for Info Sys
SP 800-60 Guide for Mapping types of info & IT to security
SP 800-70 Security configuration checklists program for IT
SP 800-137 Information security continuous monitoring

Federal Privacy Act of 1974

Computer Matching and Privacy Protection Act 1988/Amendments of 1990
OMB M-07-16 – Safeguarding PII
OMB M-06-16 – Protection of sensitive agency information

Each organization may also have specific Security guidelines and requirements such as:

HIPAA – The act defines security standards for healthcare information
DHS 4300A – Sensitive Systems Handbook 2012

ISO Standards – 27000 series for Information Security – LM is ISO 270001 certified

ISO 27001 – Specification for Information Security Management System (ISMS)
ISO 27002 – Controls and mechanisms
ISO 21827 – Characteristics of an organizations security engineering process
ISO 15408 – Common – evaluation criteria for IT security, products certified and protection

Key words indicating Cyber Security (CS) requirements/support

Access Management
Anti-tamper
Anti-virus
Application
APT
ATC
ATO
Authentication
Authorization
Availability
Big Data
BYOD
CCAO
CDTAB
C&A (certification and accreditation)
Certificate of Net Worthiness
Certification Test and Evaluation
Certified Personnel
Claims
Clearing and Sanitization Procedures
Cloud
Code Review
Common Criteria
Confidentiality
Contingency Planning
Continuous Monitoring
Critical Infrastructure
Cryptography
CUI
Cyber
Cyber Intelligence
Cyber Security
Cyber Training
Data/Content Control
Data Loss Prevention
Database
DIACAP
Disaster Recovery
DITSCAP

Forensics
Fuzzing
Gold Disk
GTI
HIPAA
IA Best Business Practice
IaaS
Incident Handling
Incident Response
Info Ops Planner
Information Assurance
Information Operations
Information Technology
Integrity
Intrusion Detection
ISSE
ITAR
Key Management
Known Threats
Malware Protection
Mission Critical
Mobile Devices
Multi-level Security (MLS)
Network
NIAP
NIPRnet/CAP
Non-repudiation
OPSEC Plan
PaaS
Patch Management
PCI
Penetration Test
Personal Data
Physical Security
PII
PPP
Privacy
Program Protection
Protection Technology

Security Management
Security Requirements
Security Risk
Security Standards
Security Test and Evalua
Security Vulnerability
SIPRnet/CAP
Software
SOX
Static Analysis
STIG
Suite B
Supply Chain
System
Threat Profiling/Modeling
TNC
Wireless, WEP, WPA, 802.11 b/g/n

Note: This list is a guideline and not an all inclusive list of CS terms

SEAM | Assurance On Demand™
Secure Engineering Assurance Model

Need help? Contact your business area security domain advocate:

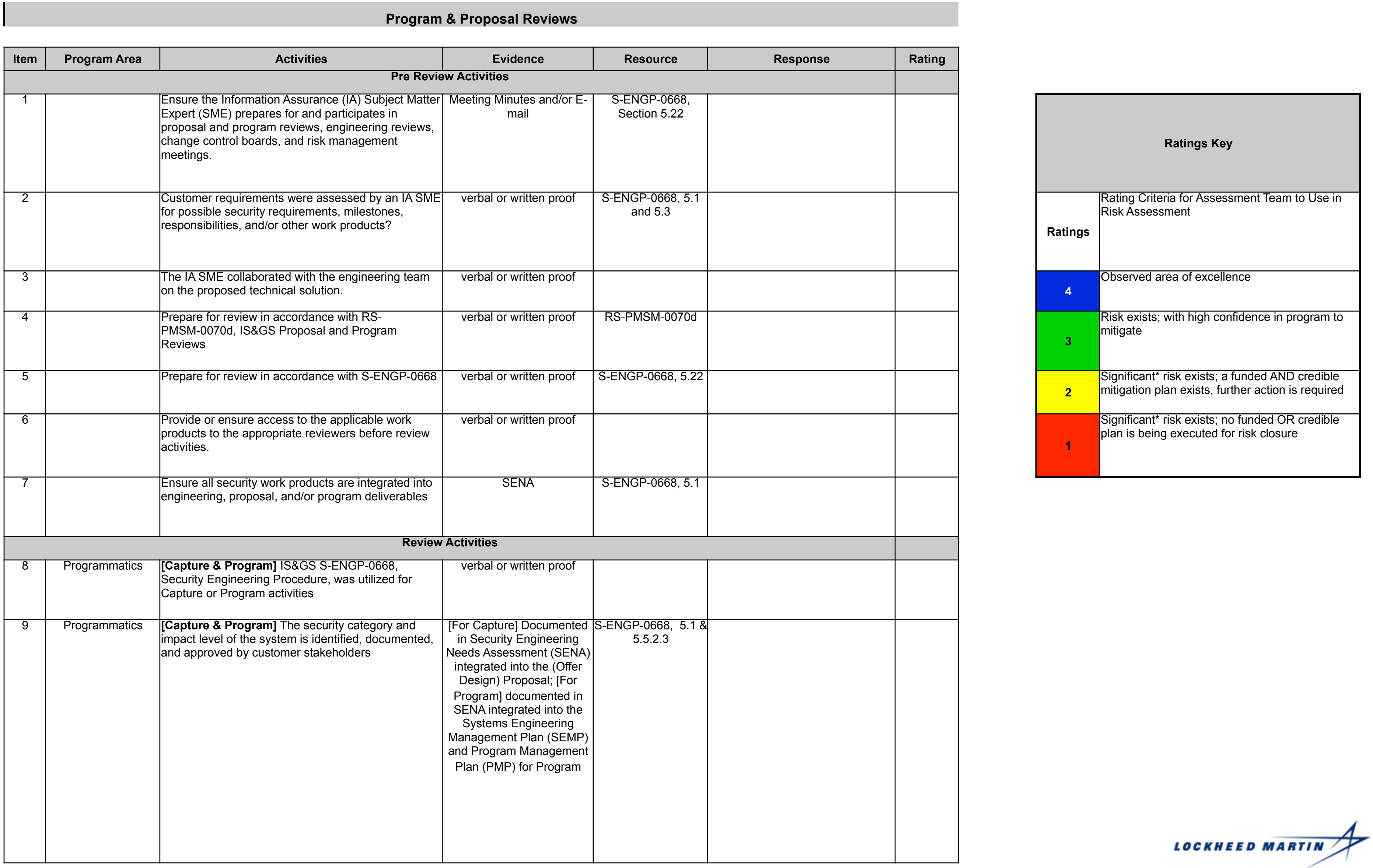
Aero - Ben Calloni
Aero – Gerry Ourada
Aero - Phillip Todd
CIS - Penny Beierschmitt
CIS - Michael Muckin
IS&GS - Dawn Beyer
IS&GS - Perri Nejib
MST - Charles Tracey
MST – John Halpin
MST - Thomas Plummer
MST – Bharat Shah
Space - Jason Blaine
Space - Daryl Spano

LM specific security references:

RS-ENGP-0044, *Systems Security*
S-ENGP-0668, *Security Engineering Procedure*

For additional terms refer to:
CNSSI 4009 – National IA Glossary

Sample from Security Assessment Tool



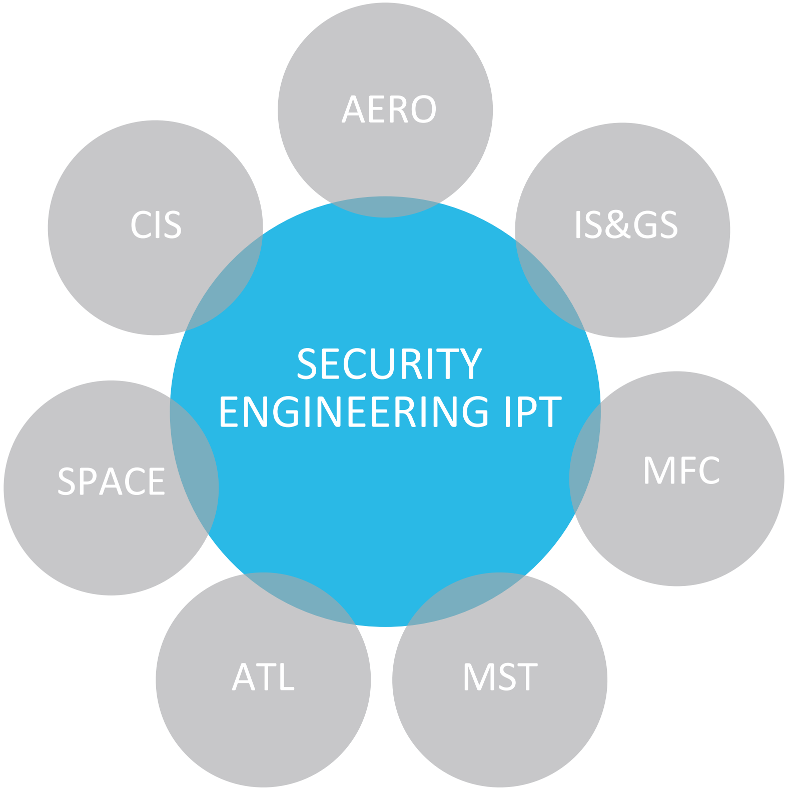
Program & Proposal Reviews

Item	Program Area	Activities	Evidence	Resource	Response	Rating
Pre Review Activities						
1		Ensure the Information Assurance (IA) Subject Matter Expert (SME) prepares for and participates in proposal and program reviews, engineering reviews, change control boards, and risk management meetings.	Meeting Minutes and/or E-mail	S-ENGP-0668, Section 5.22		
2		Customer requirements were assessed by an IA SME for possible security requirements, milestones, responsibilities, and/or other work products?	verbal or written proof	S-ENGP-0668, 5.1 and 5.3		
3		The IA SME collaborated with the engineering team on the proposed technical solution.	verbal or written proof			
4		Prepare for review in accordance with RS-PMSM-0070d, IS&GS Proposal and Program Reviews	verbal or written proof	RS-PMSM-0070d		
5		Prepare for review in accordance with S-ENGP-0668	verbal or written proof	S-ENGP-0668, 5.22		
6		Provide or ensure access to the applicable work products to the appropriate reviewers before review activities.	verbal or written proof			
7		Ensure all security work products are integrated into engineering, proposal, and/or program deliverables	SENA	S-ENGP-0668, 5.1		
Review Activities						
8	Programmatics	**[Capture & Program]** IS&GS S-ENGP-0668, Security Engineering Procedure, was utilized for Capture or Program activities	verbal or written proof			
9	Programmatics	**[Capture & Program]** The security category and impact level of the system is identified, documented, and approved by customer stakeholders	[For Capture] Documented in Security Engineering Needs Assessment (SENA) integrated into the (Offer Design) Proposal; [For Program] documented in SENA integrated into the Systems Engineering Management Plan (SEMP) and Program Management Plan (PMP) for Program	S-ENGP-0668, 5.1 & 5.5.2.3		

Ratings Key	
Ratings	Rating Criteria for Assessment Team to Use in Risk Assessment
4	Observed area of excellence
3	Risk exists; with high confidence in program to mitigate
2	Significant* risk exists; a funded AND credible mitigation plan exists, further action is required
1	Significant* risk exists; no funded OR credible plan is being executed for risk closure

Security Engineering Domain Advocates

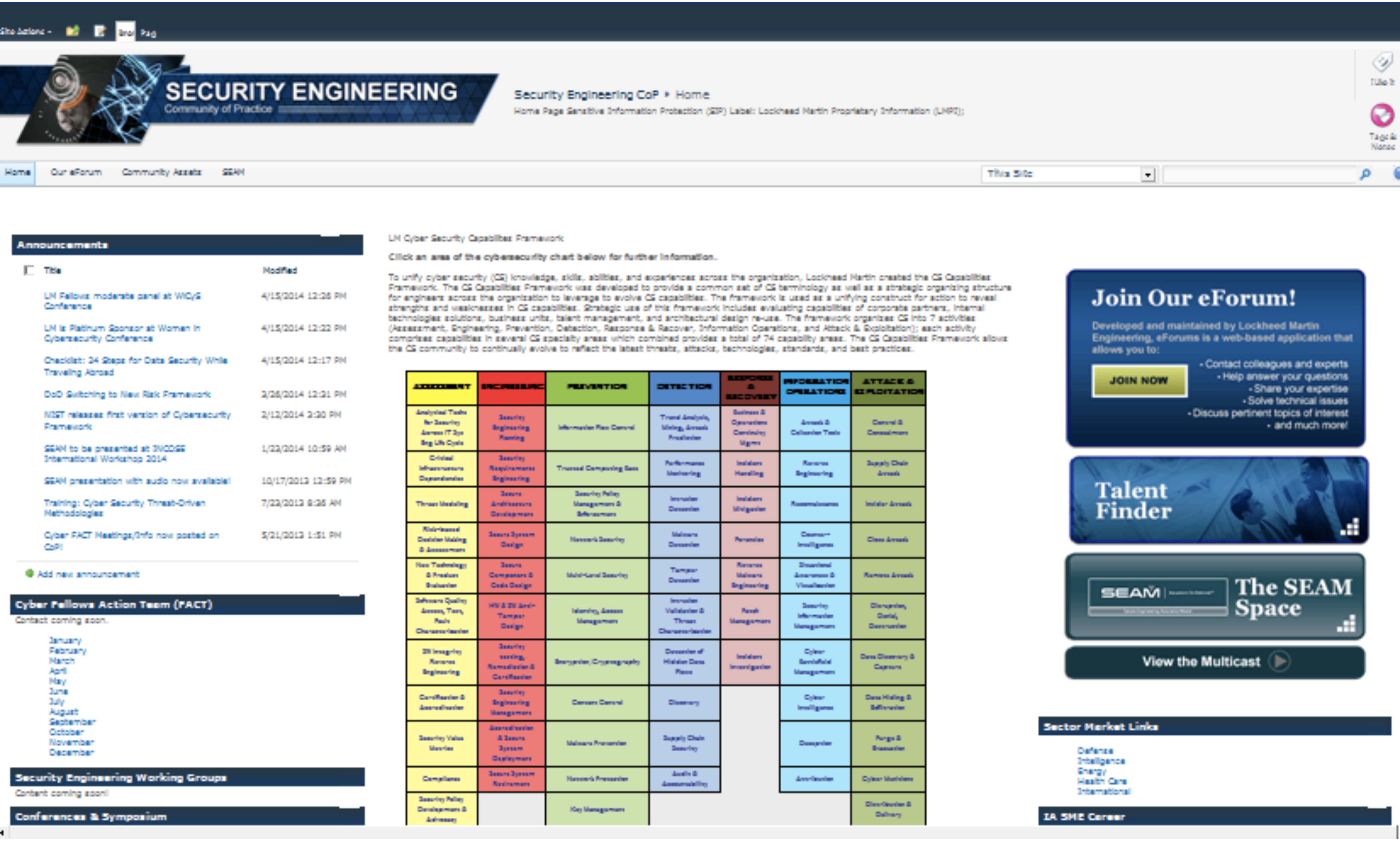
LOCKHEED MARTIN



- Security Engineering IPT in place to foster communication & collaboration across all business areas security focused SMEs
- IPT used to develop, review and communicate system security engineering efforts (eg. Security procedure, standards, SEAM tools)

- Various eForums, portals and groups for outreach
    - LM Security Engineering Community of Practice
    - Info-Assurance eForum
    - Cyber Fellows Action Team(FACT) eForum
    - AT COE
    - Secure SW Engineering eForum
    - Info System Security WG

Security Engineering CoP Portal



Security Engineering CoP ▸ Home

Home Page Sensitive Information Protection (SIP) Label: Lockheed Martin Proprietary Information (LMPI);

Announcements

□ Title	Modified
LM Fellows moderate panel at WiCyS Conference	4/15/2014 12:26 PM
LM is Platinum Sponsor at Women in Cybersecurity Conference	4/15/2014 12:22 PM
Checklist: 24 Steps for Data Security While Traveling Abroad	4/15/2014 12:17 PM
DoD Switching to New Risk Framework	3/26/2014 12:31 PM
NIST releases first version of Cybersecurity Framework	2/12/2014 3:30 PM
SEAM to be presented at INCOSE International Workshop 2014	1/22/2014 10:59 AM
SEAM presentation with audio now available!	10/17/2013 12:59 PM
Training: Cyber Security Threat-Driven Methodologies	7/22/2013 8:36 AM
Cyber FACT Meetings/Info now posted on CoP!	5/21/2013 1:51 PM

Add new announcement

Cyber Fellows Action Team (FACT)

Contact coming soon.

January
February
March
April
May
June
July
August
September
October
November
December

Security Engineering Working Groups

Content coming soon!

Conferences & Symposium

LM Cyber Security Capabilities Framework

Click an area of the cybersecurity chart below for further information.

To unify cyber security (CS) knowledge, skills, abilities, and experiences across the organization, Lockheed Martin created the CS Capabilities Framework. The CS Capabilities Framework was developed to provide a common set of CS terminology as well as a strategic organizing structure for engineers across the organization to leverage to evolve CS capabilities. The framework is used as a unifying construct for action to reveal strengths and weaknesses in CS capabilities. Strategic use of this framework includes evaluating capabilities of corporate partners, internal technologies solutions, business units, talent management, and architectural design re-use. The framework organizes CS into 7 activities (Assessment, Engineering, Prevention, Detection, Response & Recover, Information Operations, and Attack & Exploitation); each activity comprises capabilities in several CS specialty areas which combined provides a total of 74 capability areas. The CS Capabilities Framework allows the CS community to continually evolve to reflect the latest threats, attacks, technologies, standards, and best practices.

ASSESSMENT	ENGINEERING	PREVENTION	DETECTION	RESPONSE & RECOVERY	INFORMATION OPERATIONS	ATTACK & EXPLOITATION
Analytical Tools for Security Across IT Sys Eng Life Cycle	Security Engineering Planning	Information Flow Control	Trend Analysis, Mining, Attack Prediction	Business & Operations Continuity Mgmt	Attack & Collection Tools	Control & Concealment
Critical Infrastructure Dependencies	Security Requirements Engineering	Trusted Computing Base	Performance Monitoring	Incident Handling	Reverse Engineering	Supply Chain Attack
Threat Modeling	Secure Architecture Development	Security Policy Management & Enforcement	Intrusion Detection	Incident Mitigation	Reconnaissance	Insider Attack
Risk-based Decision Making & Assessment	Secure System Design	Network Security	Malware Detection	Forensics	Counter-Intelligence	Close Attack
New Technology & Product Evaluation	Secure Component & Code Design	Multi-Level Security	Tamper Detection	Reverse Malware Engineering	Situational Awareness & Visualization	Remote Attack
Software Quality Assess, Test, Fault Characterization	HW & SW Anti-Tamper Design	Identity, Access Management	Intrusion Validation & Threat Characterization	Patch Management	Security Information Management	Disruption, Denial, Destruction
SW Integrity Reverse Engineering	Security testing, Remediation & Certification	Encryption, Cryptography	Detection of Hidden Data Flows	Incident Investigation	Cyber Battlefield Management	Data Discovery & Capture
Certification & Accreditation	Security Engineering Management	Content Control	Discovery		Cyber Intelligence	Data Hiding & Exfiltration
Security Value Metrics	Accreditation & Secure System Deployment	Malware Prevention	Supply Chain Security		Deception	Purge & Destruction
Compliance	Secure System Retirement	Network Protection	Audit & Accountability		Attribution	Cyber Munitions
Security Policy Development & Advocacy		Key Management				Distribution & Delivery

Join Our eForum!

Developed and maintained by Lockheed Martin Engineering, eForums is a web-based application that allows you to:

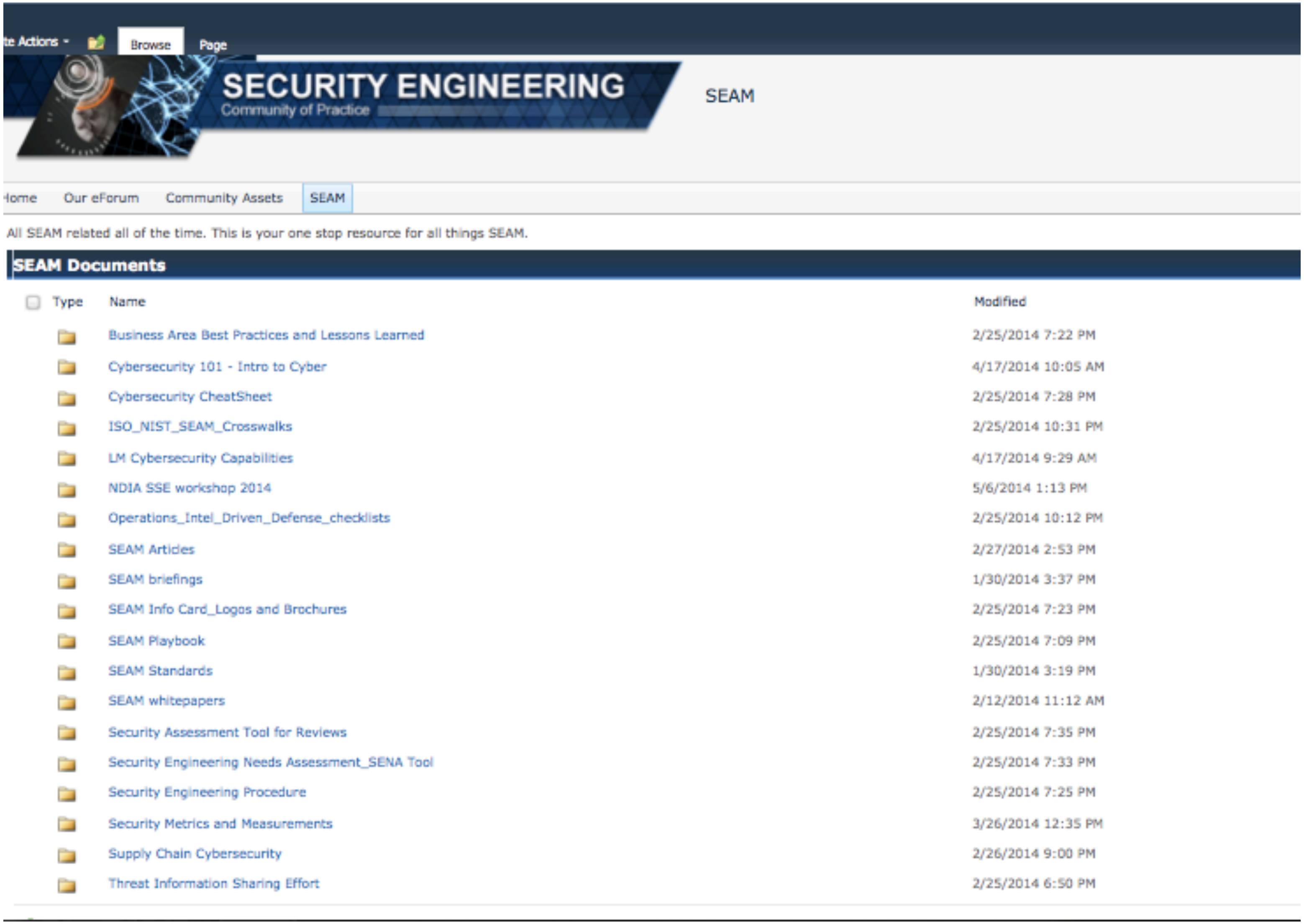
- Contact colleagues and experts
- Help answer your questions
- Share your expertise
- Solve technical issues
- Discuss pertinent topics of interest
- and much more!

Sector Market Links

Defense
Intelligence
Energy
Health Care
International

IA SME Career

SEAM™ Demo

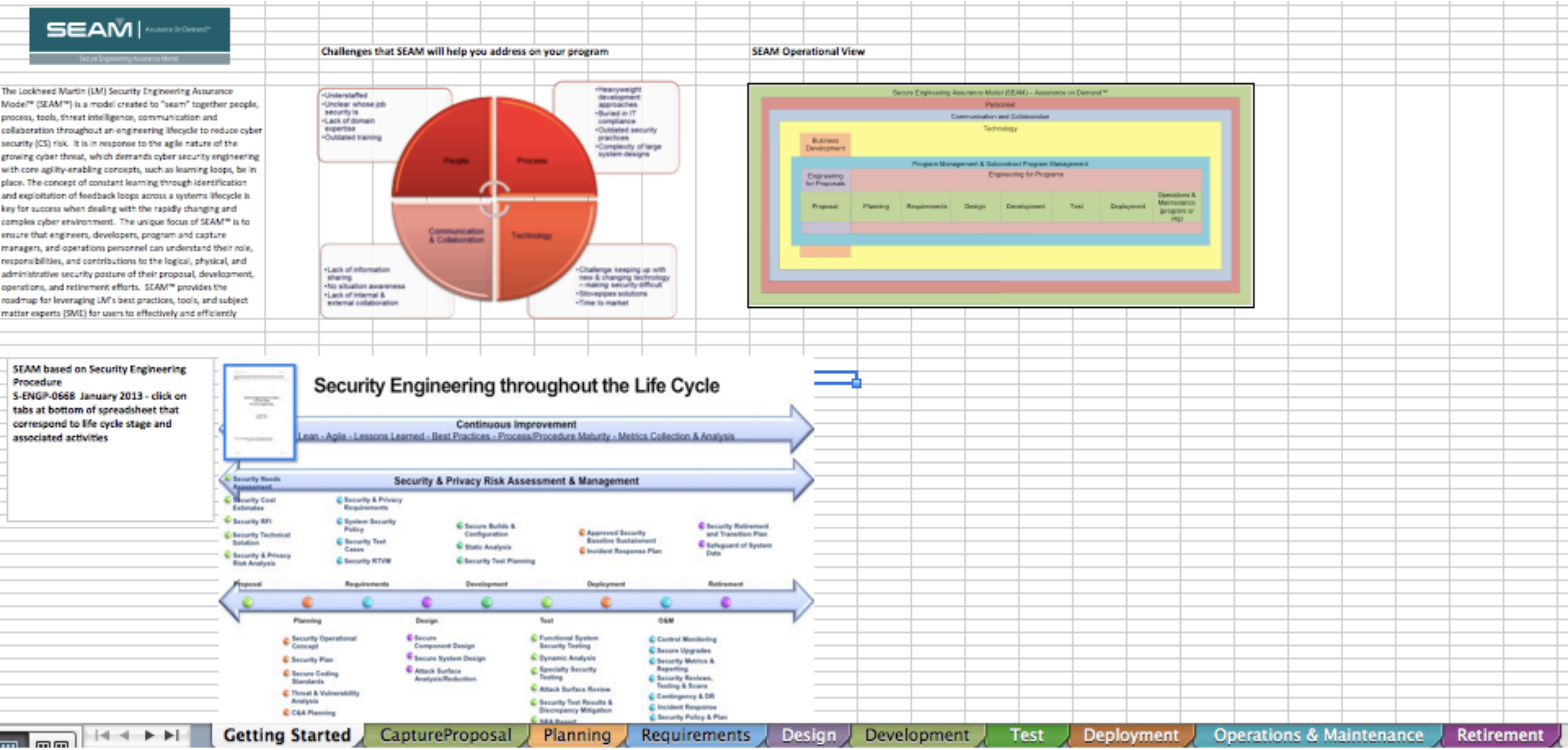


All SEAM related all of the time. This is your one stop resource for all things SEAM.

SEAM Documents

□ Type	Name	Modified
📁	Business Area Best Practices and Lessons Learned	2/25/2014 7:22 PM
📁	Cybersecurity 101 - Intro to Cyber	4/17/2014 10:05 AM
📁	Cybersecurity CheatSheet	2/25/2014 7:28 PM
📁	ISO_NIST_SEAM_Crosswalks	2/25/2014 10:31 PM
📁	LM Cybersecurity Capabilities	4/17/2014 9:29 AM
📁	NDIA SSE workshop 2014	5/6/2014 1:13 PM
📁	Operations_Intel_Driven_Defense_checklists	2/25/2014 10:12 PM
📁	SEAM Articles	2/27/2014 2:53 PM
📁	SEAM briefings	1/30/2014 3:37 PM
📁	SEAM Info Card_Logos and Brochures	2/25/2014 7:23 PM
📁	SEAM Playbook	2/25/2014 7:09 PM
📁	SEAM Standards	1/30/2014 3:19 PM
📁	SEAM whitepapers	2/12/2014 11:12 AM
📁	Security Assessment Tool for Reviews	2/25/2014 7:35 PM
📁	Security Engineering Needs Assessment_SENA Tool	2/25/2014 7:33 PM
📁	Security Engineering Procedure	2/25/2014 7:25 PM
📁	Security Metrics and Measurements	3/26/2014 12:35 PM
📁	Supply Chain Cybersecurity	2/26/2014 9:00 PM
📁	Threat Information Sharing Effort	2/25/2014 6:50 PM

SEAM™ "Playbook"



SEAM | Assurance On Demand™

Secure Engineering Assurance Model

The Lockheed Martin (LM) Security Engineering Assurance Model™ (SEAM™) is a model created to "seam" together people, process, tools, threat intelligence, communication and collaboration throughout an engineering lifecycle to reduce cyber security (CS) risk. It is in response to the agile nature of the growing cyber threat, which demands cyber security engineering with core agility-enabling concepts, such as learning loops, be in place. The concept of constant learning through identification and exploitation of feedback loops across a systems lifecycle is key for success when dealing with the rapidly changing and complex cyber environment. The unique focus of SEAM™ is to ensure that engineers, developers, program and capture managers, and operations personnel can understand their role, responsibilities, and contributions to the logical, physical, and administrative security posture of their proposal, development, operations, and retirement efforts. SEAM™ provides the roadmap for leveraging LM's best practices, tools, and subject matter experts (SME) for users to effectively and efficiently

Challenges that SEAM will help you address on your program

- Understaffed
- Unclear whose job security is
- Lack of domain expertise
- Outdated training

- Heavyweight development approaches
- Buried in IT compliance
- Outdated security practices
- Complexity of large system designs

- Lack of information sharing
- No situation awareness
- Lack of internal & external collaboration

- Challenge keeping up with new & changing technology – making security difficult
- Stovepipes solutions
- Time to market

SEAM Operational View

Secure Engineering Assurance Model (SEAM) – Assurance on Demand™
Personnel
Communication and Collaboration
Technology
Business Development
Program Management & Subcontract Program Management
Engineering for Proposals
Engineering for Programs
Proposal
Planning
Requirements
Design
Development
Test
Deployment
Operations & Maintenance (program or org)

SEAM based on Security Engineering Procedure S-ENGP-0668 January 2013 - click on tabs at bottom of spreadsheet that correspond to life cycle stage and associated activities

Security Engineering throughout the Life Cycle

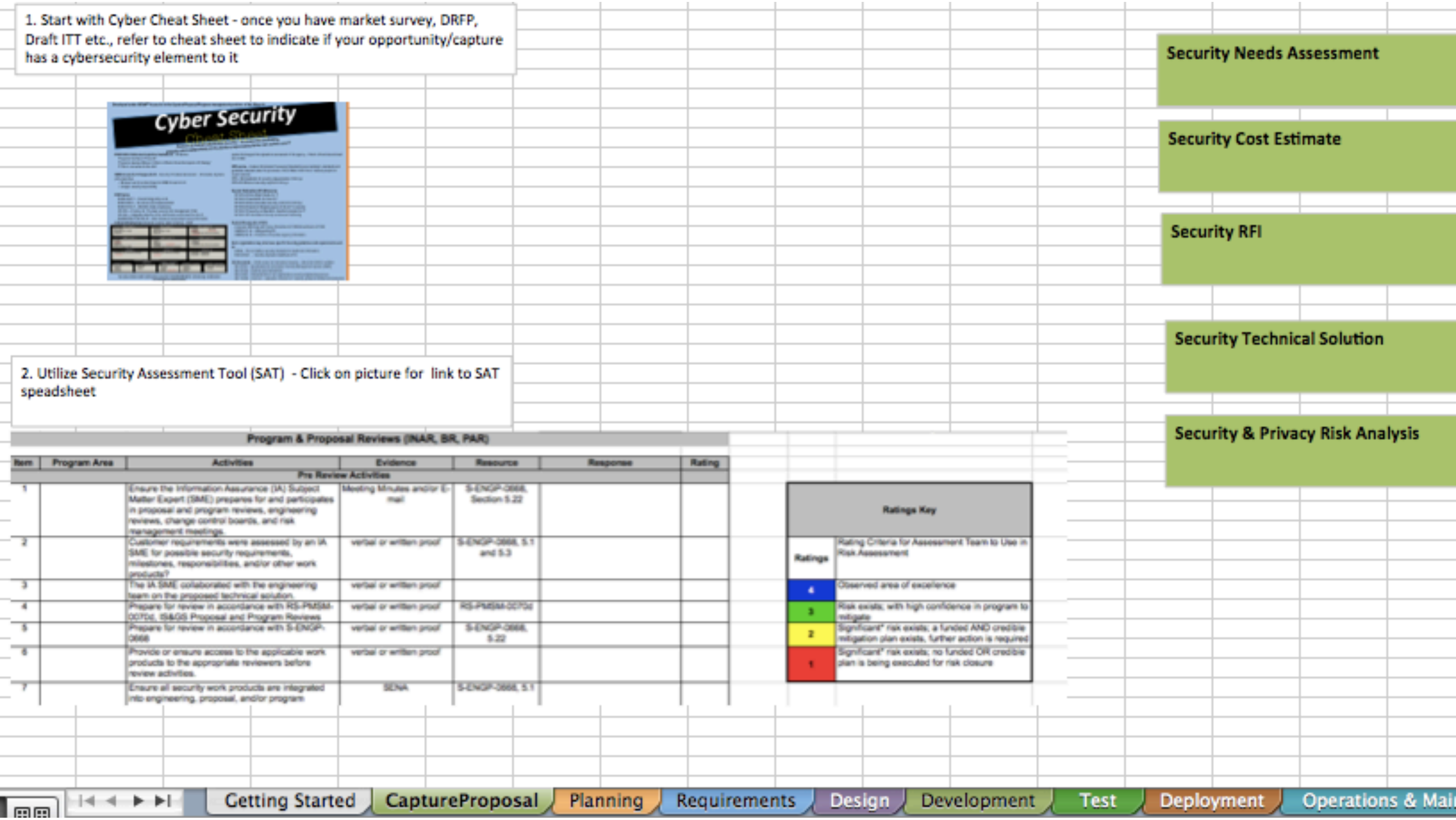
Continuous Improvement

Lean - Agile - Lessons Learned - Best Practices - Process/Procedure Maturity - Metrics Collection & Analysis

Security & Privacy Risk Assessment & Management

Proposal
Security Needs Assessment
Security Cost Estimates
Security RFI
Security Technical Solution
Security & Privacy Risk Analysis
Planning
Security Operational Concept
Security Plan
Secure Coding Standards
Threat & Vulnerability Analysis
C&A Planning
Requirements
Security & Privacy Requirements
System Security Policy
Security Test Cases
Security RTVM
Design
Secure Component Design
Secure System Design
Attack Surface Analysis/Reduction
Development
Secure Builds & Configuration
Static Analysis
Security Test Planning
Test
Functional System Security Testing
Dynamic Analysis
Specialty Security Testing
Attack Surface Review
Security Test Results & Discrepancy Mitigation
SRA Report
Deployment
Approved Security Baseline Sustainment
Incident Response Plan
O&M
Control Monitoring
Secure Upgrades
Security Metrics & Reporting
Security Reviews, Testing & Scans
Contingency & DR
Incident Response
Security Policy & Plan
Retirement
Security Retirement and Transition Plan
Safeguard of System Data

SEAM™ Playbook



1. Start with Cyber Cheat Sheet - once you have market survey, DRFP, Draft ITT etc., refer to cheat sheet to indicate if your opportunity/capture has a cybersecurity element to it

Cyber Security Cheat Sheet

2. Utilize Security Assessment Tool (SAT) - Click on picture for link to SAT speadsheet

Program & Proposal Reviews (INAR, BR, PAR)

Item	Program Area	Activities	Evidence	Resource	Response	Rating
Pre Review Activities						
1		Ensure the Information Assurance (IA) Subject Matter Expert (SME) prepares for and participates in proposal and program reviews, engineering reviews, change control boards, and risk management meetings.	Meeting Minutes and/or E-mail	S-ENGP-0668, Section 5.22		
2		Customer requirements were assessed by an IA SME for possible security requirements, milestones, responsibilities, and/or other work products?	verbal or written proof	S-ENGP-0668, 5.1 and 5.3		
3		The IA SME collaborated with the engineering team on the proposed technical solution.	verbal or written proof			
4		Prepare for review in accordance with RS-PMSM-0070d, IS&GS Proposal and Program Reviews	verbal or written proof	RS-PMSM-0070d		
5		Prepare for review in accordance with S-ENGP-0668	verbal or written proof	S-ENGP-0668, 5.22		
6		Provide or ensure access to the applicable work products to the appropriate reviewers before review activities.	verbal or written proof			
7		Ensure all security work products are integrated into engineering, proposal, and/or program	SENA	S-ENGP-0668, 5.1		

Ratings Key	
Ratings	Rating Criteria for Assessment Team to Use in Risk Assessment
4	Observed area of excellence
3	Risk exists; with high confidence in program to mitigate
2	Significant* risk exists; a funded AND credible mitigation plan exists, further action is required
1	Significant* risk exists; no funded OR credible plan is being executed for risk closure

Security Needs Assessment

Security Cost Estimate

Security RFI

Security Technical Solution

Security & Privacy Risk Analysis

perri.nejib@lmco.com
dawn.m.beyer@lmco.com