Systems Engineering Requirements Analysis and Trade-off for Trusted Systems and Networks Tutorial

Presentation

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Paul Popick

Johns Hopkins University Applied Physics Lab

Distribution Statement A – Approved for public release by OSR on 3/15/13; SR# 13-S-1385 applies.

Agenda

- **Introduction**
- **Program Protection**
- **Critical Program Information**
- **Trusted Systems and Networks**
  - Criticality Analysis
  - Threat Analysis
  - Vulnerability Assessment
  - Risk Assessment
  - Countermeasures Selection
  - Preparing the SWA Table
- **Request for Proposal (RFP) and the Program Protection Plan (PPP)**

Learning Objectives

- Describe the trusted systems and networks requirements analysis to address supply chain and malicious insertion threats
- Show the risk-based cost-benefit trade to select supply chain and malicious insertion countermeasures and requirements (risk mitigations)
- Describe basic supply chain and malicious insertion protections to incorporate in the early phase requirements definition and RFP
- Recognize that supply chain and malicious insertion program protections are a shared government-industry responsibility

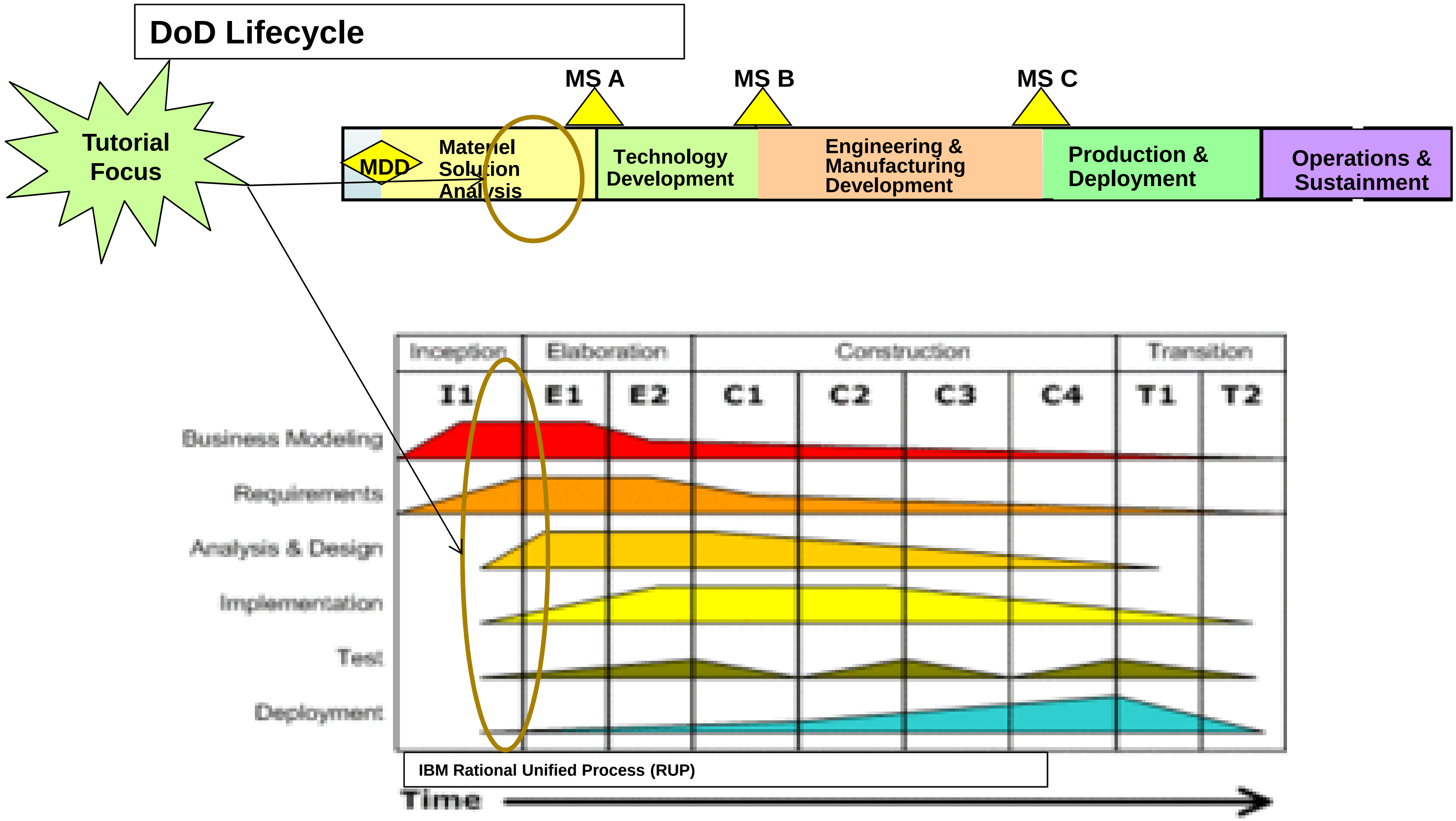
Ensuring Confidence in Defense Systems

- ***Threat*: Nation-state, terrorist, criminal, or rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Traditional Consequences*: Loss of critical data and technology**
- ***Emerging Consequences*: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; loss of confidence in critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

Tutorial Focuses on early stage of Acquisition/Development Lifecycle



Tutorial Interrelationship With 15288-Standard Processes

Agreement Processes

- **Acquisition**
- **Supply**

Organizational Project-Enabling Processes

- Life Cycle Model Management
- Infrastructure Management
- Project Portfolio Management
- **Human Resources Management**
- Quality Management

Project Processes

- Project Planning
- Project Assessment and Control
- Decision Management
- **Risk Management**
- Configuration Management
- Information Management
- Measurement

Technical Processes

- **Stakeholder Requirements Definition**
- **Requirements Analysis**
- **Architectural Design**
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

Legend: Green Primary focus of tutorial

Legend: Blue: secondary focus of tutorial

Early Phase System Security Engineering (SSE) Challenges

Ensuring that basic development, design, and supply chain requirements are selected to prevent ,detect, and respond to malicious attacks

- **Prevent – Countermeasures that reduce the exploitation of development, design, and supply chain vulnerabilities**
- **Detect – Countermeasure that monitor, alert, and capture data about the attack**
- **Respond – Countermeasures that analyze attacks and alter system or processes to mitigate the attack**

Early Phase Program Protection Plans should contain all three types of countermeasures as well as plans for more detailed program protection analysis and updates to inform system security engineering early in the design

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	**Components**	**Information**
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	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	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

Protecting Warfighting Capability Throughout the Lifecycle

Program Protection Integrated in Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39

DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

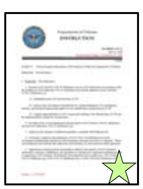
- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to <u>vulnerabilities in system design</u> or <u>subversion of mission critical functions or components</u>

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain



DoDI 8500.01E Information Assurance

- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

☆ - Update underway

Program Protection Guidance

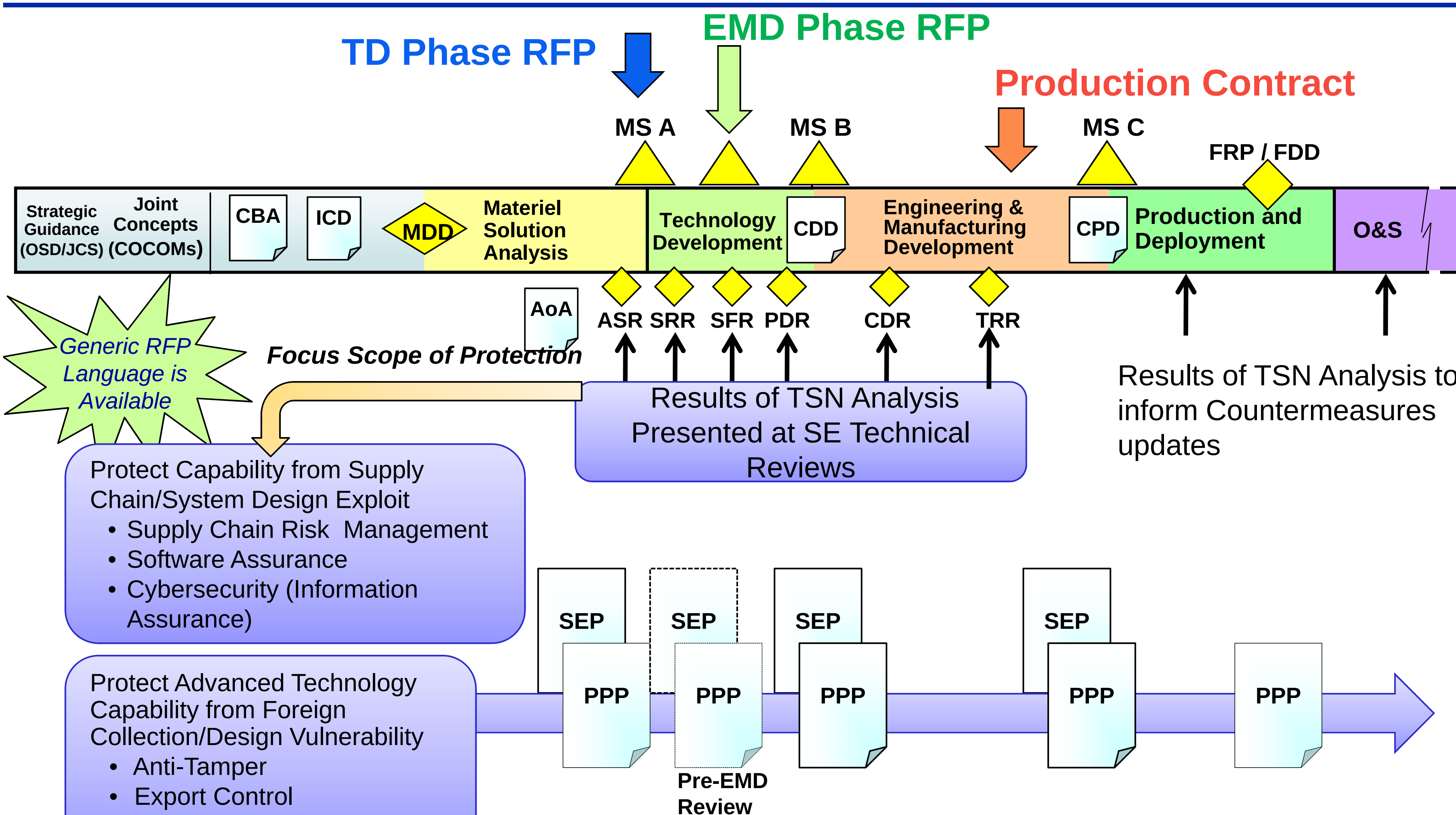
Program Protection Plan Outline & Guidance, dated 18 Jul 2011

- **Focal point for documenting Program security activities, including:**
  - Plans for identifying and managing risk to CPI and critical functions and components
  - Responsibilities for execution of comprehensive program protection
  - Tables of actionable data, not paragraphs of boilerplate
  - End-to-end system analysis and risk management
- **http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf**

Defense Acquisition Guidebook Chapter 13, "Program Protection"

- **Provides implementation guidance for TSN Analysis and CPI Protection**
- **Describes SSE activities throughout the Defense Acquisition Life Cycle**
- **https://acc.dau.mil/dag13**

PPP Development and Updates



Emphasizing Use of Affordable, Risk-Based Countermeasures

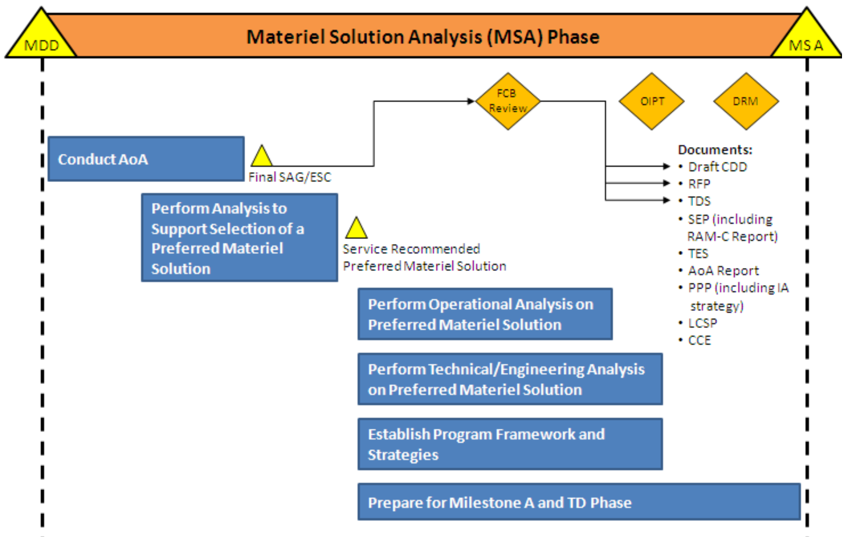
PPP Analysis Level of Detail through the Life Cycle (SETR)

	ASR	SRR	SFR	PDR	CDR	SVR/FCA
System Specification Level	• ICD / Comments on Draft CDD (if avail) • Prelim System Performance Spec • Sys model/arch including CONOPS, i/f, & operational/ functional requirements	• System Performance Spec • Verifiable sys req'ts detailed to enable functional decomposition • Req. traceability • External i/f documented	• Functional Baseline • System functions decomposed and mapped to System elements • Sys elements defined • Preliminary allocation of functions optimized	• Allocated Baseline • Preliminary design (fct and i/f) for all elements (HW & SW) complete • HW – Verifiable component characteristics • SW – CSCs, CSUs	• Initial Product Baseline • Detailed design & i/f for comp/unit production and test • HW– Physical (form fit, function) • SW– CSU level design	• SVR– System performance verified to meet functional & allocated baselines • Product Baseline for initial production
Criticality Analysis (CA)	Mission based functions	System requirements level functions	Subsystem level subfunctions	Assembly/ component	Component/ part	Part (prelim)
Vulnerability Assessment (VA)	Response to tutorial questions	System function level response to tutorial questions	Subsystem level responses	Assembly / Component level responses	component level responses	Part level responses (prelim)
Risk Assessment (RA)	• Objective risk criteria established • Applied at function level	• Risk criteria updated • applied at system level	Risk criteria updated & applied at subsystem level	Risk criteria updated & applied at assembly level	Risk criteria updated & applied at component level	Risk criteria updated & applied at prelim part level of critical components
Counter-measure (CM)	Risk based supply chain, design and SW CM in RFP	Risk based system function level CM selection	Risk based subsystem function level CM selection	Risk based assembly level CM selection	Risk based component level CM selection	Risk based part level CM selection
IA / Cyber security	• System Categorization/Registration • Initial Controls & tailoring	Risk based control strength of implementation determined	• IA Control trace to spec • Additional IA Controls tailoring/trades as CM if needed	• IA Control trace to spec • Additional IA Controls as CM if needed • IA/IA enabled Components ID'd as CM	• IA controls incorporated traced to physical baseline • Controls Assessed and discrepancies ID'd/categorized	• IA controls incorporated traced to product baseline • IAVM program established for IA control maintenance
RFP	• CM and IA controls incorporated into TD SOW and SRD		CM and IA controls incorporated into EMD SOW and SRD		CM and IA controls incorporated into Production SOW and SRD	

PPP Analysis Level of Detail through the Life Cycle (Milestones)

	Milestone A	Pre-EMD	Milestone B	Milestone C	FRP/PCA/FDD
PPP Analysis	Same level as ASR analysis	Same level as SRR and SFR	Same level as PDR	Same level as CDR and SVR	• PCA – Established Product Baseline • Critical function component bill of material (BOM)
Criticality Analysis (CA)	"	"	"	"	Part
Vulnerability Assessment (VA)	"	"	"	"	Part level responses
Risk Assessment (RA)	"	"	"	"	Risk criteria updated & applied at BOM level critical components
Countermeasure (CM)	"	"	"	"	Risk based part level CM selection
IA / Cyber security	"	"	"	"	• IA controls incorporated traced to product baseline and BOM • IAVM program established for IA control maintenance
RFP	• CM and IA controls incorporated into TD SOW and SRD	CM and IA controls incorporated into EMD SOW and SRD		CM and IA controls incorporated into Production SOW and SRD	

MSA (early) Phase Systems Engineering / Technical Analysis



Draft MSA model from OSD Development Planning Working Group, June 2012.

MSA Phase Engineering Analysis Objectives

- Confirm CONOPS and develop mission and functional threads
- Develop draft system requirements and notional system design
- Identify critical technology elements
- Determine external interfaces and interoperability requirements
- Identify critical functions and CPI

Feeds key Milestone A Requirements

- RFP, SEP (including RAM-C report), TDS, TES, PPP, LCSP, Component Cost Estimate

Influences Draft CDD development

- Balances capability, cost, schedule, risk, and affordability

Requires an adequately resourced and experienced Technical Staff

- System and Domain Engineers
- Cost Analysts
- Mission and Operations Reps

Cybersecurity
(Formerly "Information Assurance")

Assess Risks
- Vulnerabilities
- Threats
- Criticality

Apply Countermeasures

Assess Effectiveness & Residual Risks

Risk Decision/ Authorize and Sustain System

Categorize System and Information for consequence of loss in:

Confidentiality	High	MED	LOW
Integrity	High	MED	LOW
Availability	High	MED	LOW

- Security Controls Selection / Implementation
- Security Requirements development /SSE
- Component Selection / SCRM
- SRGs, STIGS, SCGs*, NIAP Evaluation
- PKI/PKE and Identity Management
- Cross Domain Solutions (UCDMO)
- UC Approved Products List
- Contractor System Security
- Lifecycle Monitoring
- Solicitations (SOO/SOW/SRD/CDRLs, ...)

- Security Controls Assessment (Compliance vs. Cat. 1, 2, 3 discrepancies)
- Developmental Test and Evaluation (T&E)/Security T&E
- Operational T&E (Pen testing, Log Demo/SCRM, etc.)

- Authorization to Operate (ATO)
- Continuous Monitoring
- Lifecycle Configuration Management
- Sustainment/IAVMs
- Periodic Re-Authorizations

Federal Statutes & Regulations

- 44 USC 3541 et. Seq. (FISMA)
- 40 U.S.C. 1401 et seq. (CCA / OMB Circular A-130)
- NSD-42 (Sec. of Nat. Sec. Telcom & IS)
- CNSSP 22 (IA Risk Mgt. for NSS)
- CNSSI 1253 (Sec. Cat. & Ctl. Sel. for NSS) / 1253A (overlays)
- …

DoD / IC Regulations

- DoD 5000 series (Acquisition)
- DoDI 5200.39 (CPI Protection)
- DoDI 5200.44 (Trusted Systems & Networks)
- DoD 8500 series (Cybersecurity)
- DoDI 8510.01 (RMF for DoD IT)
- DoDI 8551.1 (Ports Protocols & Svc)
- DoDI 8520.2 PKI/PKE
- DODI 8520.3 Identity Authentications for IS
- CJCSI 6510.1 (IA and Support to CND)
- ICD-503 (IC Risk Mgt., Cert. & Accreditation)
- …

Federal & DoD Guidance/Tools

- CNSSI-4009 (National IA Glossary)
- NIST SP 800-37 (Guide for Apply RMF)
- NIST SP 800-39 (Mgmt. of Info. Sec. Risks)
- NIST SP-800-53 (Recommended Security Controls
- NIST SP 800-53A (Assessing Sec. Controls)
- Draft NIST SP 800-160 System Security Engineering)
- https://diacap.iaportal.navy.mil/ks/Pages/default.aspx
- http://www.disa.mil/Services/Information-Assurance/SCM/EMASS
- http://www.dmea.osd.mil/trustedic.html
- …

* SRG – Security Requirements Guides
STIG – Security Technical Implementation Guides
SCG – Security Configuration Guides

Program Protection Analysis

<u>CPI Analysis</u> – Threat of Technology Loss

- Identify CPI
- Determine CPI Risk
- Protect CPI

Tutorial Focus

<u>TSN Analysis</u> - Threat of system & supply chain malicious insertion

- Criticality Analysis
- Threat Analysis
- Vulnerability Assessment
- Cybersecurity (IA) Assessment

↔

- Risk Assessment
- Countermeasures selection
- Software Assurance
- Hardware Assurance

Critical Program Information (CPI)

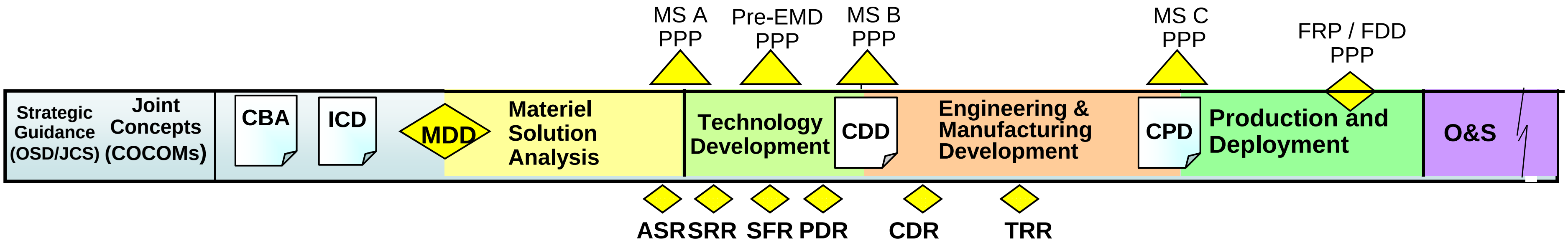
- **What is CPI?**
  – US capability elements that contribute to the warfighters' technological advantage throughout the life cycle, which if compromised or subject to unauthorized disclosure, decrease the advantage. US capability elements may include but are not limited to technologies and algorithms residing on the system, its training equipment, or maintenance support equipment.*

- **Why protect CPI?**
  – Delay technology loss, and our adversary's ability to reverse engineer or re-engineer U.S. technology, to maintain our technological advantage to the greatest extent practicable

CPI includes only the elements:
(1) providing a capability advantage and
(2) residing on the system or supporting systems.

****Department of Defense Instruction (DoDI) 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, and Acquisition (RDA) Programs," Expected approval 1st Quarter FY14***

Critical Program Information (CPI) 3-Step Analysis



1. Identify CPI

- Gather data to support CPI identification (e.g., intelligence on foreign capabilities)
- Perform technical analysis to identify CPI
- Review and approve CPI

2. Assess CPI Risk

- Determine criticality of CPI
- Request counterintelligence reports to understand threats
- Determine exposure of CPI

3. Protect CPI

- Select and implement CPI countermeasures

Identify, Assess, and Protect CPI concurrently throughout the acquisition lifecycle. Iterate these steps prior to development or update of the PPP for each phase.

Step 1: Identify CPI

- **Gather data to support CPI identification**
  - Assess the state of science and technology to gauge the US technological advantage for the desired capability
  - Obtain intelligence on foreign capabilities and exports
  - Identify advanced capabilities provided by another acquisition program, subsystem, or project that will be incorporated or implementing into your program – inherited CPI
- **Perform technical analysis to identify organic CPI**
  - Convene a Systems Security Engineering / Program Protection Working Group
  - Use CPI decision aids and tools which may include the Defense Science & Technologies List (DSTL), the Army Critical Technologies Toolkit, CPI Survey Questionnaire (DON), DoDI S-5230.28, Provisos

WG Members
Program Manager
Science & Technology
Security w/ Intel/CI reach-back
Systems Engineer

- **Review and approve CPI**
  - Program Manager and the Program Executive Office (if applicable)

A determination of what is CPI must be made regularly throughout the lifecycle, with input from multiple subject matter experts.

Each Service may have more granular process and/or tools for identifying CPI.

An Element may be CPI if it…

- **Was identified as CPI previously by your program or another program (horizontal identification)**
- **Has been modernized / improved / enhanced**
- **Involves a unique method, technique, or application that cannot be achieved using alternate methods and techniques**
- **Performance depends on a unique, specific production process or procedure**
- **Depends on technology that was adjusted/adapted/calibrated during testing and there is no other way to extrapolate usage/function/application**
- **…AND the element provides a clear warfighting technological advantage**

Consider the complete system when identifying CPI
(e.g., subsystems, mission packages, and interdependent systems)

Defense Acquisition Guidebook 13.3.1

Is it CPI?

- An algorithm developed in 1970 that has been published in a major research journal
- A unique technology only available to the U.S. military that no other country possesses
- COTS hardware and software
- A technology being exported
- A technology previously identified as CPI by another program

Step 2: Determine CPI Risk

- **Determine <u>criticality</u> of CPI based on intelligence**
  - What capabilities and technologies does the adversary possess?
  - What capabilities and technologies is the adversary developing or will possess?
  - Is there a US warfighter technological advantage?
  - How long do we expect the US warfighter technological advantage to last?

  Technology Targeting Risk Assessment (TTRA)

- **Request counterintelligence reports to understand <u>threats</u> to CPI**
  - What capabilities, systems, information, and technologies are being targeted?
  - How capable is the adversary in collecting information?
  - What counterintelligence support will be provided to the program?

  Counterintelligence Support Plan (CISP)

- **Determine the <u>exposure</u> of CPI**
  - Will the system be sold or exported (Direct Commercial Sales or Foreign Military Sales)?
  - Where will the system be used? (CONUS or OCONUS)

Determine CPI Risk

CPI	Impact on US Military Advantage	Investment (Time and Money)
CPI #1	Moderate	Moderate
CPI #2	Very High	Moderate

Criticality
Very High
High
Moderate
Low
Very Low

Consequence

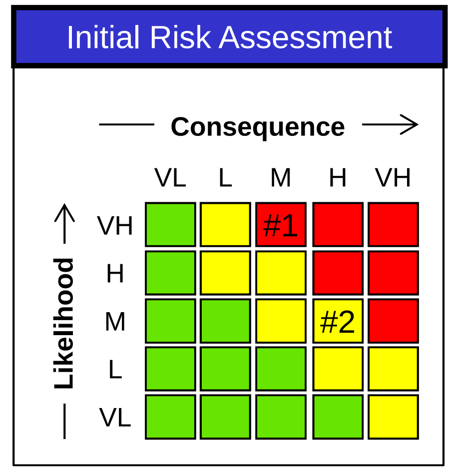
CPI	Foreign Adversary Skill	Foreign Interest
CPI #1	Very High	High
CPI #2	Moderate	High

Threat
Very High
High
Moderate
Low
Very Low

CPI	Export	Operational Environment	Number of Samples	Vulnera-bilities
CPI #1	Yes	N/A	High	High
CPI #2	No	OCONUS	Low	Moderate

Exposure
Very High
High
Moderate
Low
Very Low

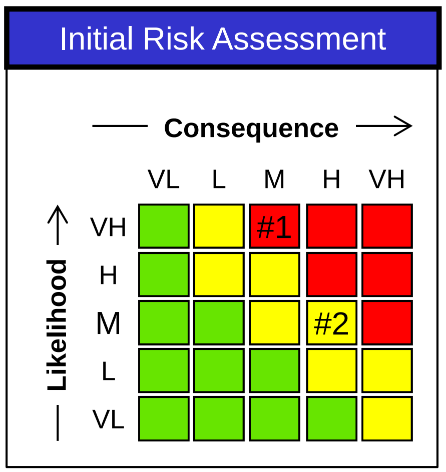
Likelihood



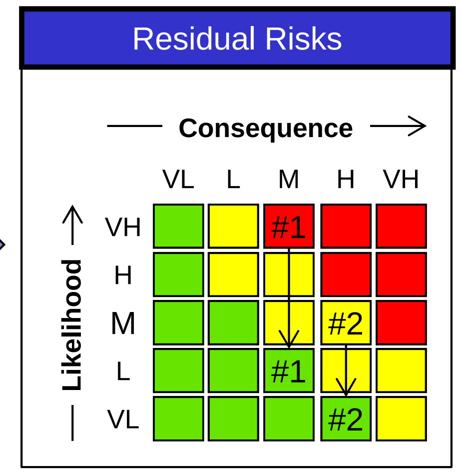
Work In Progress – The DoD 5200.39-Manual Working Group will be reviewing and further defining this methodology.

Determine the level of risk associated with each CPI based on criticality, threat, and exposure

Step 3: Protect CPI
Select/Implement CPI Countermeasures

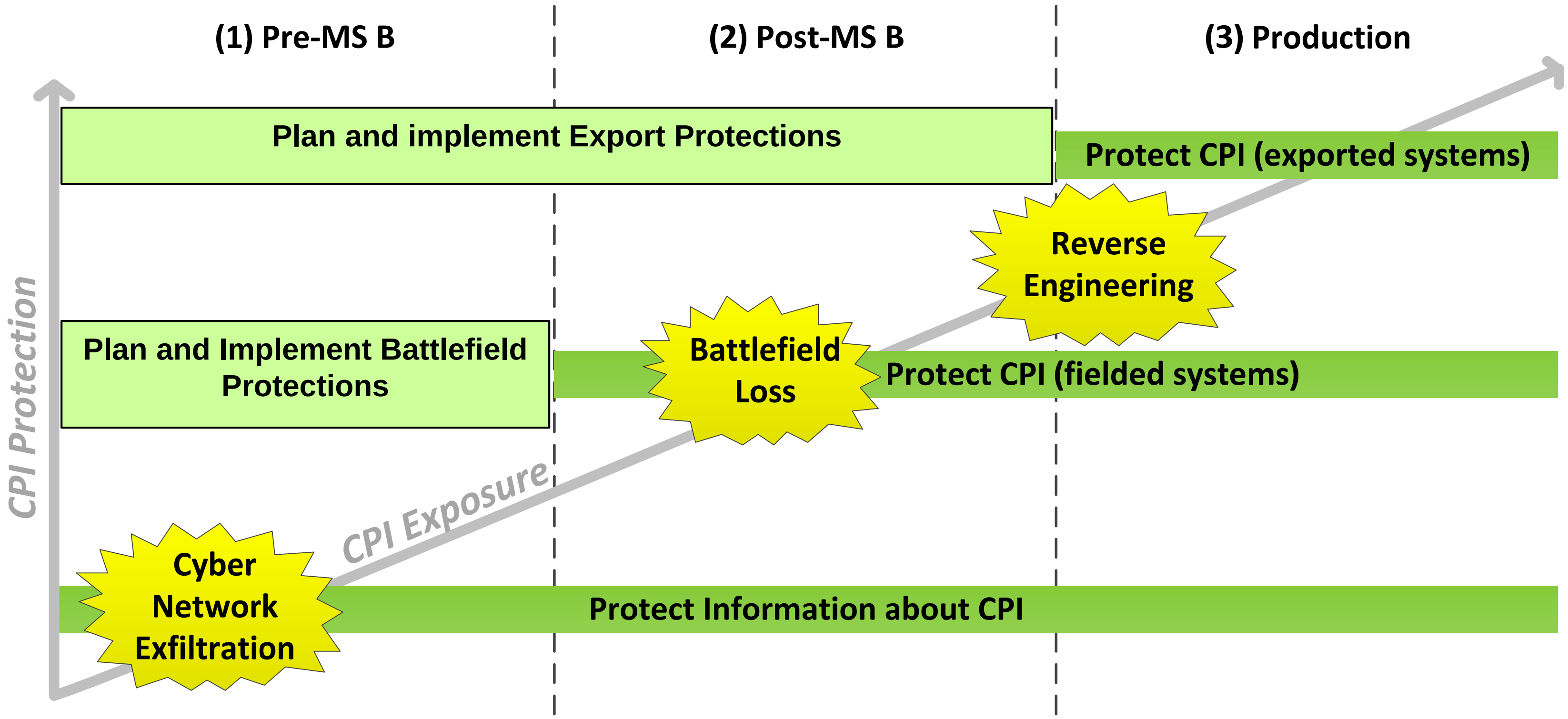


	Countermeasure
Required	Anti-Tamper
	Communications Security
Exports only	Defense Exportability Features (DEF)
Exports only	Foreign Disclosure / Agreement
	Information Assurance
	Operations Security
	Personnel Security
	Physical Security
	Software Assurance
	Transportation Management



Select countermeasures to decrease the likelihood the CPI will be lost; Implement by flowing countermeasures into SOW and System Requirements Document (SRD)

Lifecycle Considerations



Implement countermeasures throughout the lifecycle based on criticality / consequence of loss and likelihood from threats and exposure

CPI Analysis-Related Program Protection Plan Sections

- **Section 2.0 Program Protection Summary**
  - Summary list of CPI and corresponding countermeasures
- **Section 3.0 CPI and Critical Components**
  - Organic & inherited CPI and consequence of compromise
- **Section 4.0 Horizontal Protection**
  - Other programs with same or similar CPI
- **Section 5.0 Threats, Vulnerabilities, and Countermeasures**
  - Details on CPI threats, vulnerabilities, and countermeasures
- **Section 7.0 Program Protection Risks**
  - Describe overall initial and residual risks
- **Section 8.0 Foreign Involvement**
  - Foreign involvement and exposure
  - Defense exportability features
- **Appendix B: Counterintelligence Support Plan (CISP)**
- **Appendix D: Anti-Tamper Plan**

Table 2.2-1: CPI and Critical Components Countermeasure Summary

	#	Protected Item (Inherited and Organic)	Countermeasures 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CPI	1	Algorithm QP	X	X	X	X	X	X	X		X					X	X	
CPI	2	System Security Configuration											X			I		
CPI	3	Encryption Hardware	X	X	X	X	X	X	X	X				X		X		
CPI	4	IDS Policy Configuration	X	X	X	X	X	X	X	X						X		
CPI	5	IDS Collected Data	X	X	X	X	X	X	I								I	
CPI	6	KGV-136B	X	X	X	X			I		I				I			

KEY *[Examples Included: UPDATE THIS LIST ACCORDING TO PROGRAM]*

	General CMs	Research and Technology Protection CMS	Trusted Systems Design CMs
Key X = Implemented I = Denotes protection already implemented if CPI is inherited	**1** Personnel Security **2** Physical Security **3** Operations Security **4** Industrial Security **5** Training **6** Information Security **7** Foreign Disclosure/Agreement	**8** Transportation Mgmt **9** Anti-Tamper **10** Dial-down Functionality	**11** IA/Network Security **12** Communication Security **13** Software Assurance **14** Supply Chain Risk Management **15** System Security Engineering (SSE) **16** Other

EXAMPLE DATA

Note: When actual program data is entered, classify this information per the program's SCG as well as the Anti-Tamper SCG.

DoD Program Protection Plan Outline and Guidance, July 2011

Critical Program Information (CPI) Analysis & Trusted Systems and Networks (TSN) Analysis

CPI Analysis – Threat of Technology Loss

- Identify CPI
- Determine CPI Risk
- Protect CPI

Tutorial Focus

TSN Analysis - Threat of system & supply chain malicious insertion

- Criticality Analysis
- Threat Analysis
- Vulnerability Assessment
- Cybersecurity (IA) Assessment

↔

- Risk Assessment
- Countermeasures selection
- Software Assurance
- Hardware Assurance

TSN Analysis for Supply Chain and HW/SW Assurance

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

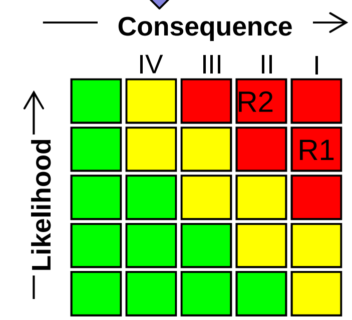
Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium

Consequence of Loss
Very High
High
Moderate
Low
Very Low

Likelihood of Loss
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Risk Assessment



Initial Risk

Identification of Potential Countermeasures

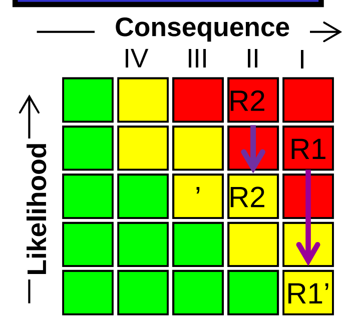
Options
Prevent CMs
Detect CMs
Respond CMs

Trade-off Analysis

Risk Mitigation Decisions

Countermeasure (CM) Selection

Risk Assessment



Mitigated Risk

TSN Analysis Related Program Protection Plan Sections

Sections

1. Introduction
2. Program Protection Summary
3. **Critical Program Information (CPI) and Critical Functions**
4. Horizontal Protection
5. **Threats, Vulnerabilities, and Countermeasures**
6. Other System Security-Related Plans and Documents
7. **Program Protection Risks**
8. Foreign Involvement
9. Processes for Management and Implementation of PPP
10. Processes for Monitoring and Reporting CPI Compromise
11. Program Protection Costs

Appendices

A. Security Classification Guide

B. Counterintelligence Support Plan

C. Criticality Analysis

- See CA Brief

D. Anti-Tamper Plan (If Applicable)

- See AT Guidance

E. Information Assurance Strategy

- See IA Strategy Guidance

- **If it is desired to attach other documents to the PPP, call them "Supporting Documents"**
  - These will not be included in the package routed up the chain for signature
- **PPP Appendix that require other signatures must be approved prior to PPP approval**
  - Includes SCG, CISP, AT Plan, IA Strategy

Tailor Your Plan to Your Program; Classify Tables Appropriately

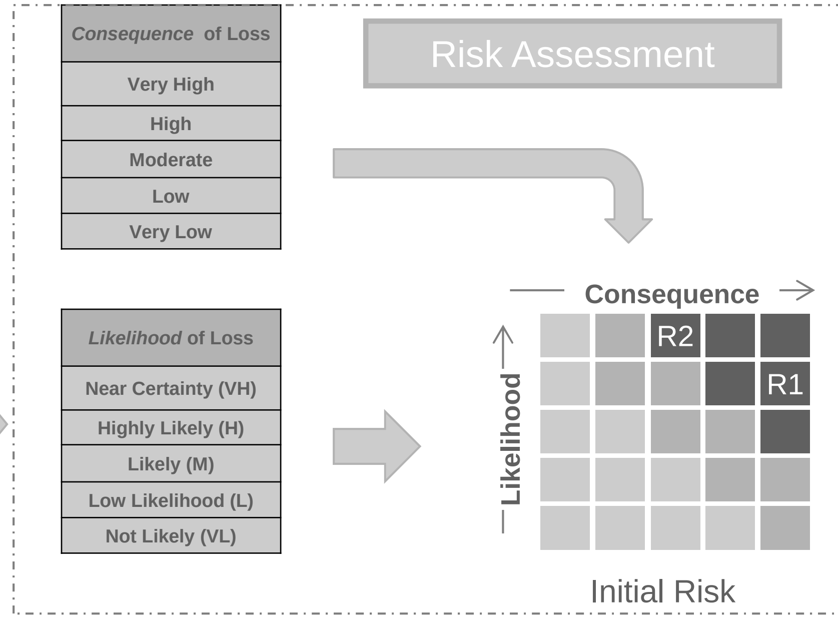
Criticality Analysis

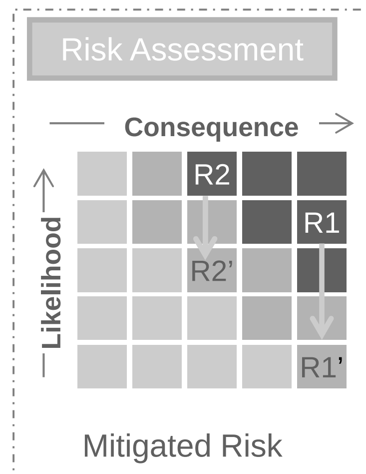
Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

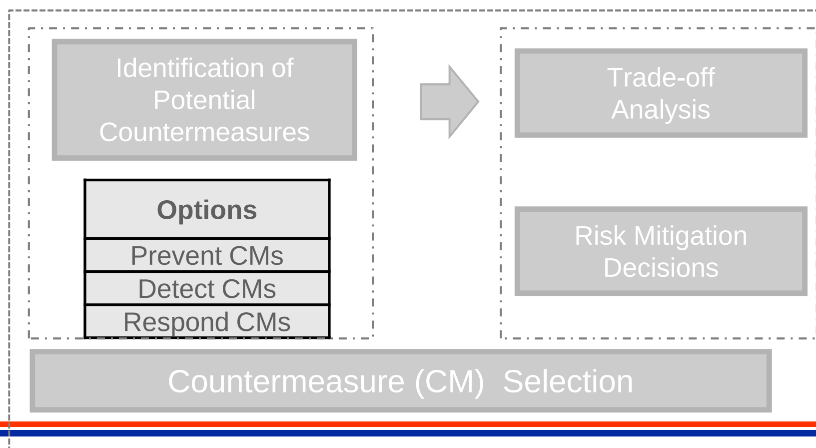
Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium







Criticality Analysis Methodology

Integral Part of SE Process

MS A Phase Inputs:
ICD
Concept of Operations
Potential Software development processes
Potential Vulnerabilities
Preferred concept

- Identify and group Mission Threads by priority

- Identify Critical Functions that will be implemented with logic bearing components
- Assign Criticality Levels

- Map Threads and Functions to Subsystems and Components

- Identify Critical Suppliers

Leverage existing mission assurance analysis, including flight & safety critical

Criticality Levels

Level I:	**Total Mission Failure**
Level II:	**Significant/Unacceptable Degradation**
Level III:	**Partial/Acceptable Degradation**
Level IV:	**Negligible**

Outputs:
- Table of Level I & II Critical Functions and Components
- TAC Requests for Information

Criticality Analysis Exercise – Scenario Description

- In this Exercise, you will perform an initial Criticality Analysis. You will determine the Critical Functions of a system, but not the implementing Critical Components.

- You have been assigned to the program office for an acquisition program that has just completed its Analysis of Alternatives (AoA) and has begun the engineering analysis of the **preferred concept** .

- The **preferred concept** is a fixed wing unmanned aircraft system (UAS) to perform an ISR mission. The program office has begun defining and decomposing the preferred concept and assessing the critical enabling technologies.

- The ISR mission thread is the "kill chain" mission thread – to consider search, locate, and track of an enemy surface strike group, and to pass targeting information back to an airborne E-2D that, in turn, provides information to a carrier strike aircraft.

Criticality Analysis Exercise – Template for Results

- Divide into teams of 2 to develop an initial Criticality Analysis
- You have been provided with
  - A concept of operations
  - A generic unmanned aerial vehicle operational view (OV-1)
  - A copy of the chart shown below to record your results
- Determine and list 5 to 6 Critical Functions associated with the "kill chain" mission thread. Concentrate on functions that will be implemented with logic bearing hardware, firmware, and software. Assign Criticality Levels.

#	Critical Function	Level
1		
2		
3		
4		
5		
6		

Criticality Analysis Exercise – Results Discussion

Brainstorm and consolidate the results provided by the whole group

#	Critical Function	Level
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Note: CA exercise results "exemplar" will be provided for use with future exercises

Threat Analysis

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

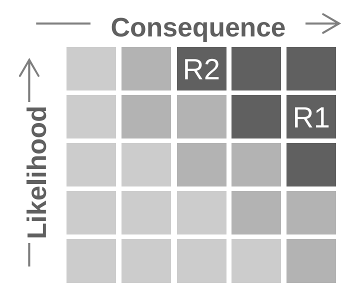
Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium

Risk Assessment

Consequence of Loss
Very High
High
Moderate
Low
Very Low

Likelihood of Loss
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)



Initial Risk

Identification of Potential Countermeasures

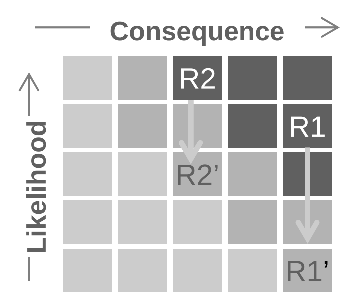
Options
Prevent CMs
Detect CMs
Respond CMs

Trade-off Analysis

Risk Mitigation Decisions

Countermeasure (CM) Selection

Risk Assessment

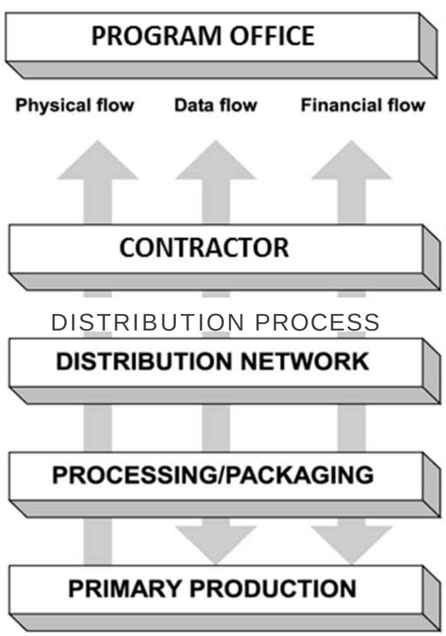


Mitigated Risk

Generic Threats – Supply Chain Attacks

Representative attacks illustrate where in the supply chain the infiltration occurs and what the malicious insertion accomplishes

Supply Chain



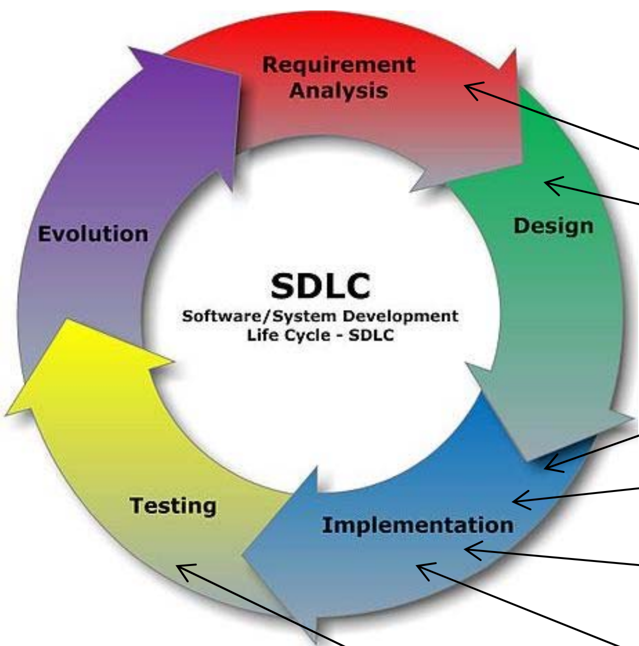
Representative Supply Chain Attacks

- Clandestine changes to mission data
- Infiltration of sites to insert back doors and malicious logic into some micro electronics (FPGAs and other devices)
- Infiltration of company receiving department to add / substitute components with backdoors to allow remote penetration during operations, denial of service, etc.
- Infiltration of transportation companies to intercept DoD component shipments (developmental or COTS) and substitute components that have malicious code inserted
- Insertion of malicious software in the open source used for math libraries
- Infiltration allowing malicious software implantation through 3rd party bundling
- Establishment of shell company to insert counterfeit parts
- Infiltration to manipulate the hardware or software baselines
- Infiltration of company software development to insert software which exfiltrates data
- Infiltration to compromise the design/fabrication of hardware

Can have multiple levels: OEMs → subassembly suppliers → assembly suppliers → integrators

Generic Threats – Malicious Insertion in the Software Development Life Cycle

Representative attacks illustrate what part of the SDLC is targeted and how malicious insertion is accomplished



Attack Vectors for Malicious Code Insertion

Hidden in software's design (or even requirements)

Appended to legitimate software code

Added to linked library functions

Added to installation programs, plug-ins, device drivers, or other support programs

Integrated into development tools (e.g., compiler generates malicious code)

Inserted via tools during system test

Generic Threats – Malicious System Exploitation Attacks

Representative Attacks and Vectors for Malicious Exploitation of Fielded Systems

Configuration, Operational Practices

Supply Chain (penetration, corruption)

Malware (downloaded, embedded)

External Mission Load Compromise

DNS Based Threats (cache poisoning)

Applications (built-in malware)

E-mail Based Threats (attachments)

Data Leakage (via social media)

Password Misuse (sharing)

Denial of Service (embedded malware)

Kill Switch Activation (embedded malware)

Mission Critical Function Alteration (embedded malware)

Exfiltration (by adversary)

Network Threat Activity (host discovery)

Compromised Server Attacks (on clients)

Malicious Activity (disruption, destruction)

Auditing Circumvention (evading detection)

Web Based Threats (disclosing sensitive info)

Zero Day Vectors (vulnerabilities without fixes)

Improper File/Folder Access (misconfiguration)

- **Supply Chain**
- **Embedded Malware**

Threat Analysis – Methodology for Potential Supplier Threats

- **Input**
  - List of critical functions and their (potential) implementing critical components
- **For each Level I and selected Level II Critical Function**
  - Determine COTS or custom development: Hardware, Software, Firmware
  - Develop a list of potential suppliers of critical functions
    - On shore, Off Shore, Reuse (Gov't or Commercial)
  - Match potential suppliers to critical components
    - Include supplier location
    - For reuse include program / system source and OEM location
- **Build potential supply chain diagrams or tables for use in Vulnerability Assessment**
- **Request supplier threat information for Level I / Level II critical-function component suppliers**
- **Output**
  - Supply chain diagrams
  - Threat request information
    - Note: Assume a Likely [M(3)] to Highly Likely [H(4)] threat likelihood for suppliers that have limited supply alternatives, can not be switched for valid reason, or have no information request results

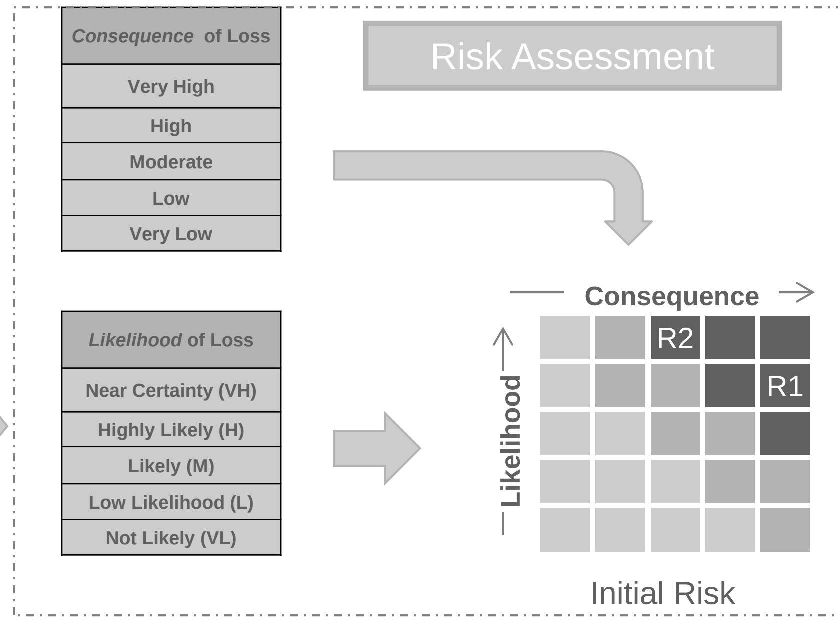
Vulnerability Assessment

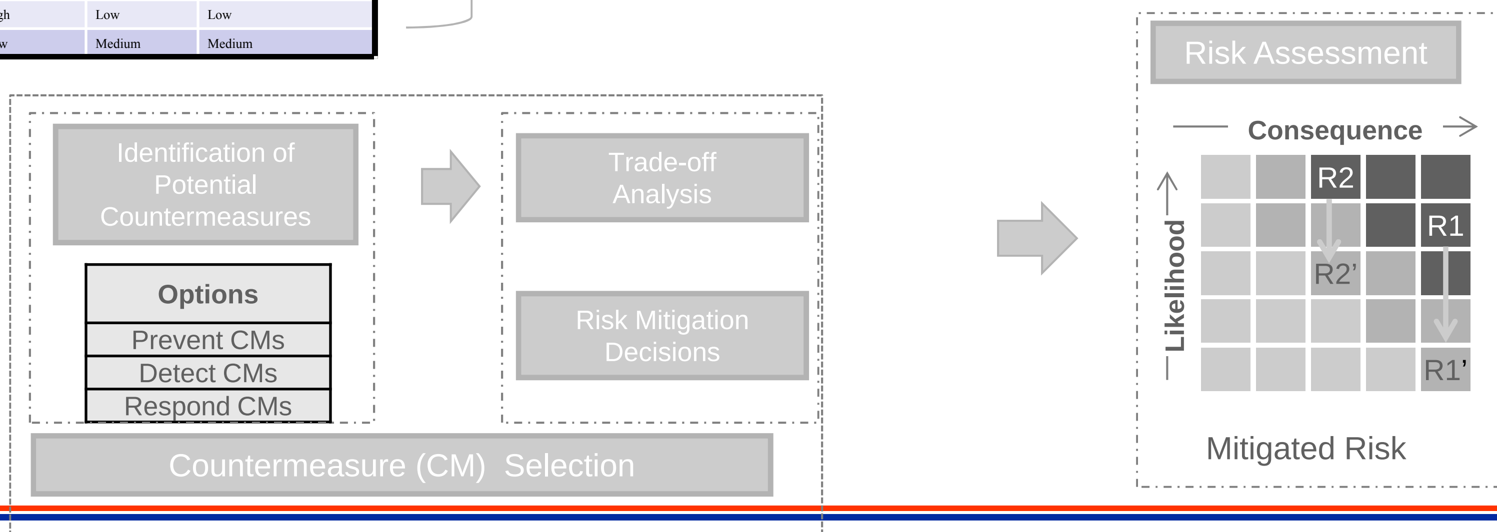
Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium





Vulnerability Assessment Methodology

Inputs:
Concept of Operations
Notional System Architecture
Critical Functions
Some Potential Critical Components
Threat Analysis Results
Descriptions of Potential Processes:

- Determine Access Path Opportunities
- Determine Attack Scenarios
- Determine Exploitable Vulnerabilities
- Inform the TA/VA-Based Risk Likelihood Determination

Fidelity increases as the system is elaborated in later phases

Outputs:
- Supply chain vulnerabilities
- HW/SW development process vulnerabilities
- System design vulnerabilities
- Input to likelihood assessment of risks
- Possible countermeasures/ mitigations

Cybersecurity (IA) Assessment Methodology

Inputs:

- Information Assurance Strategy
- System Security User Requirements from ICD / CDD and SRD if available
- Draft SOW (if available)

Identify the required system IA controls based upon system categorization

Assess vulnerabilities of IA control implementations to System and Development environment to applicable attack vectors

Assess critical function confidentiality, integrity and availability vulnerabilities (H, M, L) to applicable attack vectors

Determine which potential controls could be incorporated into the SOW and which controls could be incorporated into the SRD, and needed implementation strength

Fidelity increases as the system is elaborated in later phases

Outputs:

- IA System confidentiality, integrity & availability vulnerabilities
- Assessment of critical function confidentiality, integrity & availability vulnerabilities
- Potential list of controls to incorporate into the SRD and SOW along with implementation strength
- Trace of IA Controls to SRD and SOW

Vulnerability Assessment Exercise Part I

Continuing with the UAS for maritime surveillance, we will look at potential supply chains (including software and firmware COTS) and the software development process for the UAS search and tracking functions.

The end objective is to identify and describe potential vulnerabilities so that relevant, cost effective "countermeasures" can be selected and incorporated into the system requirements or the statement of work prior to issuing the RFP.

You have been provided with

- Criticality Analysis Results *in Exemplars*
- Architecture Handout
  - A notional architecture that is used to support requirements analysis
  - Two potential supply chains diagrams
  - Two possible software development life cycles
  - Generic supply chain and malicious insertion threats/vectors

Follow the steps on the next slide and brainstorm a list of the possible vulnerabilities associated with identified potential supply chains and possible software development lifecycles/processes. Also consider UAS-specific vulnerabilities for selected potential critical component(s).

Detailed Steps for the Vulnerability Assessment Exercise Part I

Step 1 – Determine Access Path Opportunities

- Consider the system CONOPS (including OV-1 diagram) and notional architecture to determine design-attribute related attack surfaces
- Consider the SE, SW, and Supply Chain processes for process-activity type weaknesses

Step 2 – Select Attack Scenarios

- Determine the types of attack scenarios that might apply by considering how an adversary could exploit potential software and supply chain weaknesses
- Select a set of attack vectors from the catalog that best fit the attack surface identified by the chosen attack scenarios (the "catalog" is provided by the generic threats in the Architecture Handout and a reference attack vector catalog in the Tutorial Appendix)
- Consider both intentional and unintentional vulnerabilities (keeping in mind that the exploit will be of malicious intent)

Step 3 – Determine Exploitable Vulnerabilities

- Based on the identified attack vectors that best fit the attack surface, select two critical components for each potential supply chain
- Apply each supply chain and software development attack vector against each component and, with engineering judgment, assess if the attacks are successful
- If successful, then list the associated weakness as an exploitable vulnerability
- In addition to generic vulnerabilities, consider also any UAS domain-specific vulnerabilities

Step 4 – Inform the Threat Assessment / Vulnerability Assessment Based Risk Likelihood Determination

- This step is part of the next exercise

Vulnerability Assessment Exercise Part I – Output Template

Supply Chain 1

Supply Chain Vulnerability	Software Development Vulnerability

Supply Chain 2

Supply Chain Vulnerability	Software Development Vulnerability

Vulnerability Assessment Exercise Part II – with Heuristic Questions

Continuing with the UAS for maritime surveillance, we will assess vulnerabilities in the potential supply chains and software development process for two selected critical components from Vulnerability Assessment Exercise Part I.

The end objective is to identify supply chain and software development vulnerabilities in a manner that will support quantifying the critical component risk likelihood.

You have been provided with

- Two selected potential critical components
- A set of generic supply chain and software development vulnerability questions
- Also use the results of participants' brainstorming UAS domain-specific vulnerabilities

Approach

- Use the following two critical components, one from each of the potential supply chains provided
  - CC1: FPGA (from Sub HIJ – supply chain 1)
  - CC2: Custom Tracking Algorithm SW (from Sub SSS – supply chain 2)

Vulnerability Assessment Exercise Part II

Approach, cont.

- For each component, answer a set of vulnerability questions covering
  - Supply chain (next page) and
  - Software development (second page following)
- Add domain specific questions or any questions that you developed during vulnerability brainstorming that are not already addressed by the supply chain and software development questions (third page following)
- Review each question and determine if the intent of the question applies to your acquisition. If it does not, mark it N/A. If it does, continue:
- Determine if your current vulnerability mitigation plans address the question. If so, place a "Y" in the corresponding row; if not, place a "N". (This approach assumes that plans to address the identified vulnerability are already in place.)
  - Using Q1 as an example: If one of your CC1 identified vulnerability mitigations deals with the need for a trusted supplier, then enter a "Y" in that row under the CC1 column. If not, then enter a "N"
- Note:
  - Do not be surprised if there is a large number of "N"s recorded, as access to a draft SOW, which would address many of these questions, has not been provided.

Vulnerability Assessment Exercise Part II

Potential Supply Chain Vulnerabilities

CC1	CC2	
		1. Does the Contractor have a process to establish trusted suppliers ?
		2. Does the Contractor obtain DoD specific ASICS from a DMEA approved supplier
		3. Does the Contractor employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use
		4. Does the Contractor require suppliers to have similar processes for the above questions?
		5. Has the prime contractor vet suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?
		6. Are secure shipping methods used to ship? How are components shipped from one supplier to another?
		7. Does receiving supplier have processes to verify critical function components received from suppliers to ensure that components are free from malicious insertion (e.g. seals, inspection, secure shipping, testing, etc.)?
		8. Does the supplier have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
		9. Does the supplier have controls to limit access to critical components?
		10. Can the contractor identify everyone that has access to critical components?
		11. Are Blind Buys Used to Contract for Critical Function Components?
		12. Are Specific Test Requirements Established for Critical Components?
		13. Does the Developer Require Secure Design and Fabrication or Manufacturing Standards for Critical Components?
		14.

Vulnerability Assessment Exercise Part II

CC1 CC2

Potential Software Development Vulnerabilities for critical SW

1. Has the developed established secure design and coding standards that are used for all developmental software (and that are verified through inspection or code analysis)?
   - Secure design and coding standards should considers CWE, Software Engineering Institute (SEI) *Top 10* secure coding practices and other sources when defining the standards?
2. Are Static Analysis Tools Used to Identify violations of the secure design and coding standards?
3. Are design and code inspections used to identify violations of secure design and coding standards?
4. Have common Software Vulnerabilities Been Mitigated?
   - Derived From Common Weakness Enumeration (CWE)
   - Common Vulnerabilities and Exposures (CVE)
   - Common Attack Pattern Enumeration and Classification (CAPEC)
5. Is penetration testing planned based upon abuse cases
6. Are Specific Code Test-Coverage Metrics Used to Ensure Adequate Testing?
7. Are Regression Tests Routinely Run Following Changes to Code?
8. Does the Software Contain Fault Detection/Fault Isolation (FDFI) and Tracking or Logging of Faults?
9. Is developmental software designed with least privilege to limit the number size and privileges of system elements
10. Is a separation kernel or other isolation techniques used to control communications between level I critical functions and other critical functions
11. Is a software load key used to encrypt and scramble software to reduce the likelihood of reverse engineering?
12. Do the Software Interfaces Contain Input Checking and Validation?
13. Is Access to the Development Environment Controlled With Limited Authorities and Does it Enable Tracing All Code Changes to Specific Individuals?
14. Are COTS product updates applied and tested in a timely manner after release from the software provider
15.

Vulnerability Assessment Exercise Part II

Add Brainstormed Y/N Questions to Address Any UAS Domain and Design Specific Vulnerabilities

CC1	CC2

1.
2.
3.
4.
5.
6.
7.
8.

Vulnerability Assessment Exercise Part II – Discussion

Walk through one or two student vulnerability assessment responses for each of the potential supply chains

Brainstorm possible countermeasures to the vulnerabilities identified

Discuss iterative design interactions and then provide a solution exemplar as a basis for next exercise

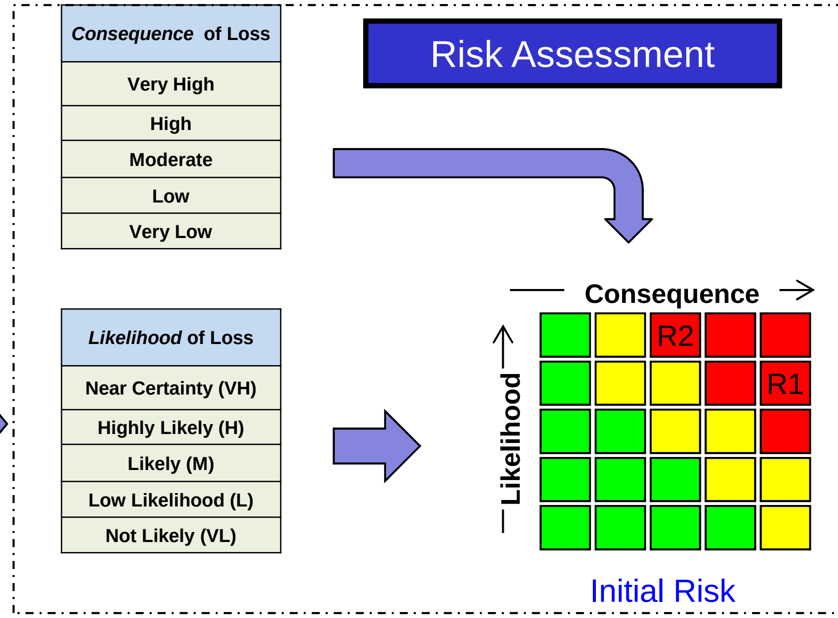
Initial Risk Assessment

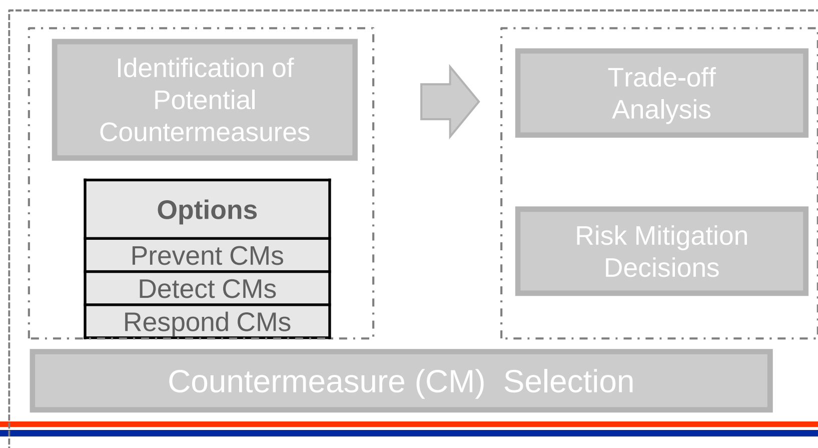
Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

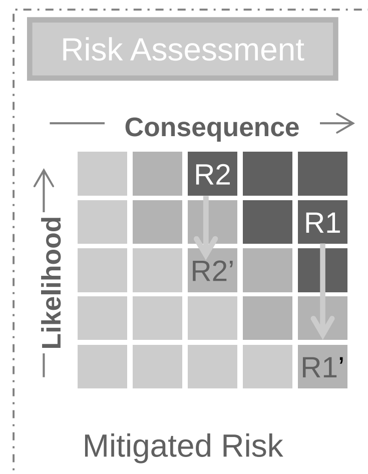
Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium







Distribution Statement A – Approved for public release by OSR on 3/15/13; SR# 13-S-1385 applies.

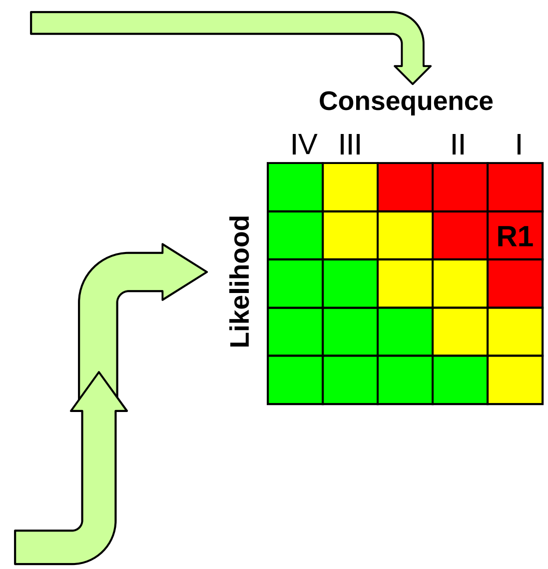
Risk Assessment Methodology

The Criticality Level (resulting from the CA) yields a consequence rating as shown:

The critical component associated with risk R1 is a Level I component.

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Initial Risk Posture



The overall likelihood rating is determined by combining the likelihood information from the Threat, Vulnerability and the Cybersecurity (IA) Assessments

The illustrated critical component risk R1 has an overall highly likely (H = 4) rating

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

The overall risk rating for R1 (designated by row–column) is: **4–5**

Risk Assessment Exercise – Overview

- In this Exercise, you will perform a risk assessment to determine a risk rating for selected critical components
- Use the CA results to determine the consequence rating
- Use the TA and VA results to determine the likelihood rating
  - Use the exemplar critical components and their associated TA and VA exercise results
  - Calculate the likelihood using the supply chain, software development, and domain-specific information for each critical component
  - Use these assessments to determine the overall risk likelihood
- Develop an overall risk rating assessment that places the critical component risk in the risk cube

- You have been provided with
  - Two selected critical components
  - VA exercise results (exemplars)
  - Copies of the output templates shown on the next slide, but with previous exemplars filled in

Risk Assessment Exercise – Templates for Results

Overall Likelihood

Component	Threat Assessment Likelihood	Supply Chain VA Likelihood	Software Development VA Likelihood	Overall Likelihood
Critical Component 1				
Critical Component 2				

Risk Rating

Component	Overall Likelihood	Consequence (from Criticality Analysis)	Risk Rating
Critical Component 1			
Critical Component 2			

Risk Assessment Exercise – Likelihood Guidance

- One approach for translating the vulnerability assessment into a risk likelihood input is to use an equal weighted scoring model that calculates the percentage of "No" answers in the groupings of "Y-N" questions from the VA.
- We will use this method for the exercise:

Number of "No" Responses	Risk Likelihood
All "NO"	Near Certainty (VH - 5)
>=75% NO	High Likely (H - 4)
>= 25% No	Likely (M - 3)
<= 25% No	Low Likelihood (L - 2)
<= 10% No	Not Likely (NL - 1)

- Use the table above to determine the risk likelihood for each critical component
  - Develop likelihood calculations for supply chain, software development, and domain-specific
- Approaches to combining the supply chain vulnerability assessment and the software vulnerability Assessment:
  - Do separate calculations to determine two vulnerability likelihoods and then use the most severe among the threat and the two vulnerabilities as the overall likelihood input
  - ✓ Do separate calculations and average to get a single likelihood calculation
  - Domain specific judgment on weightings to get a single likelihood

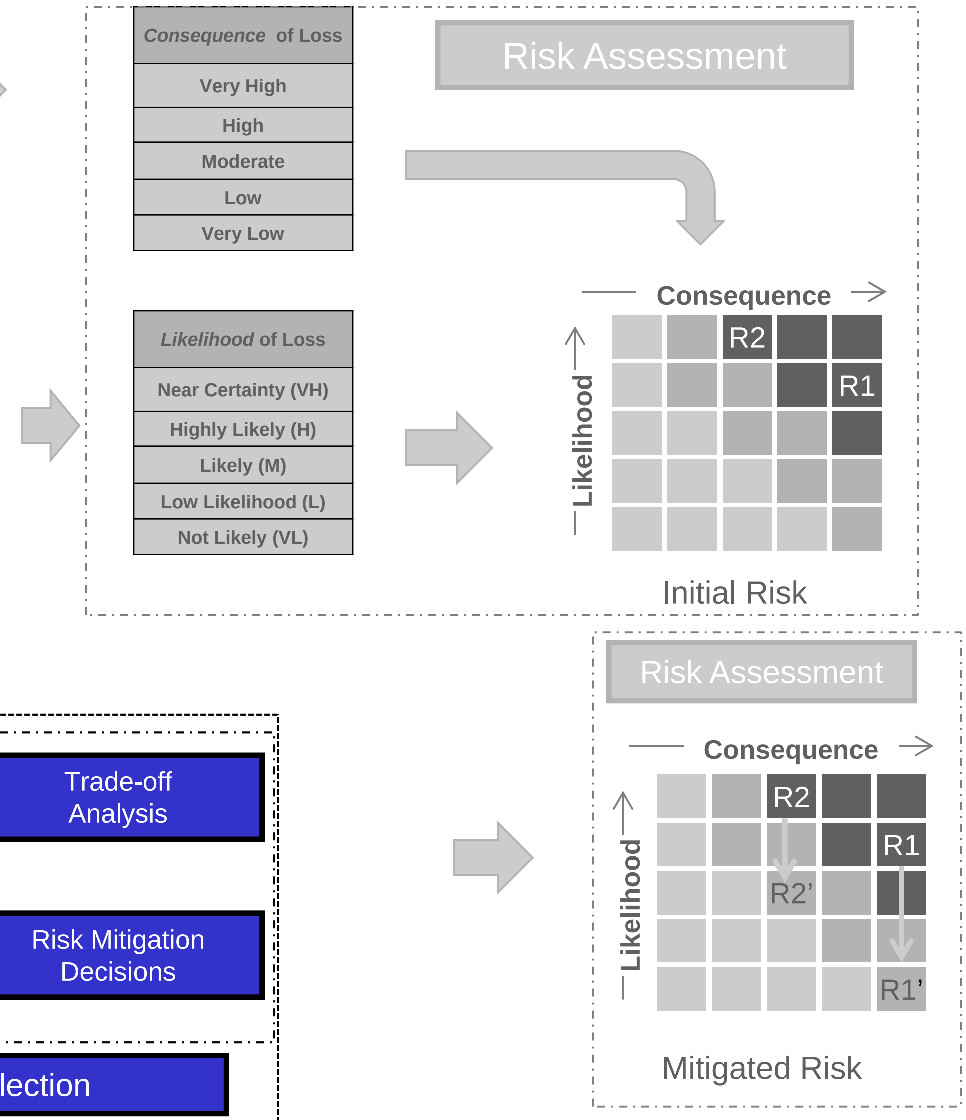
Countermeasures Selection

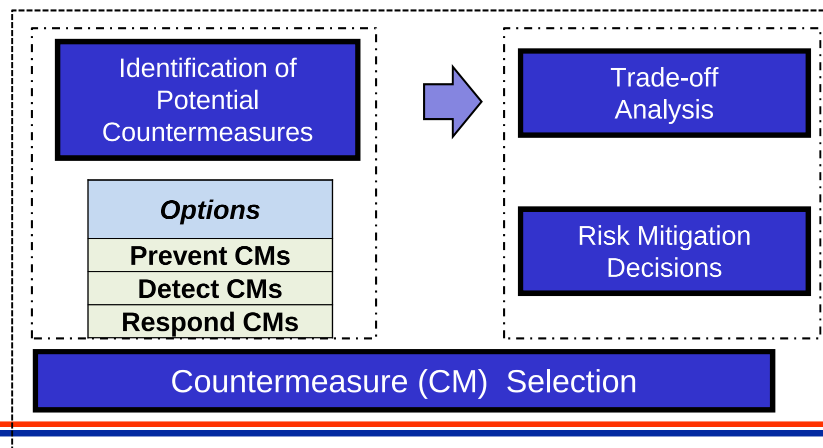
Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium





Policy and Guidance for ASICs

In applicable systems,* integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC)). – DoDI 5200.44

- PPP Outline and Guidance on Microelectronics for ASICs
  - Requires programs to identify all ASICs that require an accredited trusted supplier
  - Requires program to describe how they will make use of accredited trusted suppliers of integrated circuit-related services
- Defense Acquisition Guidebook (DAG) guidance (Chapter 13)
  - ASICs meeting policy conditions must be procured from a DMEA accredited trusted supplier implementing a trusted product flow
  - Defense Microelectronics Activity (DMEA) maintains a list of accredited suppliers on its website at http://www.dmea.osd.mil/trustedic.html.
  - Critical Design Review (CDR) criteria: Assess manufacturability including the availability of accredited suppliers for secure fabrication of Application-specific integrated circuits (ASICs), Field-programmable gate array (FPGAs), and other programmable devices

***Applicable systems**:

(1) National security systems as defined by section 3542 of title 44, United States Code (U.S.C.) (Reference (l));

(2) Mission Assurance Category (MAC) I systems, as defined by Reference (j); or

(3) Other DoD information systems that the DoD Component's acquisition executive or chief information officer determines are critical to the direct fulfillment of military or intelligence missions;

Policy and Guidance for Other Integrated Circuits

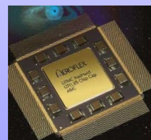
Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use. – DoDI 5200.44

- PPP Outline and Guidance on Supply Chain Risk Management:
  - Requires programs to describe how the program manages supply chain risks to CPI and critical functions and components
- PPP Outline and Guidance on Trusted Suppliers:
  - Requires program to describe how the program will make use of accredited trusted suppliers of integrated circuit-related services
- PPP Outline and Guidance on Counterfeit Prevention:
  - Requires program to describe counterfeit prevention measures and how the program will mitigate the risk of counterfeit insertion during Operations and Maintenance
- Defense Acquisition Guidebook (DAG) guidance (Chapter 13)
  - Critical Design Review (CDR) Criteria:
    - Address how the detailed system design includes and appropriately addresses security and SCRM considerations
    - Assess manufacturability including the availability of accredited suppliers for secure fabrication of ASICs, FPGAs, and other programmable devices

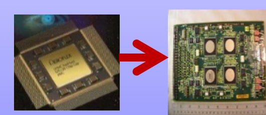
Notional Use Cases and Countermeasures for Integrated Circuits

Use Cases

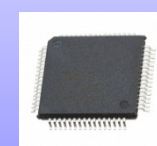
Use Case 1:
Custom ASIC that has a specific DoD military end use



Use Case 2:
ASIC in a COTS assembly that is primarily intended for commercial market



Use Case 3:
MOTS/GOTS Integrated Circuit (IC) that has a DoD end use



Countermeasures

Use Case 1:

- Use Trusted Supply Flow (Trusted Supplier) for design, mask, fabrication, packaging and testing

Use Case 2:

- Perform supply chain risk assessment of ASICs if the COTS assembly is determined as a critical component
- Implement SCRM countermeasures commensurate with assessed risk

Use Case 3:

- Consider source and employment history
- Apply countermeasures commensurate with assessed risk, including enhanced/focused testing
- Use trusted supplier and product flow as applicable, such as FPGA programming services;
- Use DMEA accredited trusted supplier and trusted product flow if ASIC

Countermeasures Based on the Vulnerability Assessment

- **There are two aspects of countermeasures selection associated with the Vulnerability Assessment results**
  - 1) How much should be invested in countermeasures; i.e., how many of them do you need and/or how high a cost should be tolerated? This question is tied to the overall risk rating (H-M-L) which, in turn, is tied to the number of “No” answers in VA Exercise Part II.
  - 2) What types of countermeasures are needed. This question is tied to the specific vulnerabilities identified in the VA Exercises and captured in the domain-specific questions of Part II.

Examples of Possible Process Countermeasures

Risk	Cost
-1	M
-2	H
-1	L
-2	L
-1	M
-2	H
-2	M
-1	L

Possible acquisition process countermeasures for critical functions with risk lowering impact and order of magnitude cost

- ❑ A supplier management plan that
  - Provides supplier selection criteria to reduce supply chain risks
  - Evaluates and maintains a list of suppliers and alternate suppliers with respect to the criteria established
  - Requires identification and use of functionally equivalent alternate components and sources
- ❑ An anonymity plan that
  - Protects the baseline design, test data, and supply chain information
  - Uses blind buys for component procurement
- ❑ Secure design and coding standards that address the most common vulnerabilities, identified in CWE and/or the CERT
- ❑ Use of the secure design and coding standards as part of the criteria for design and code inspections
- ❑ Use of static analyzer(s) to identify and mitigate vulnerabilities
- ❑ Inspection of code for vulnerabilities and malware
- ❑ Access controls that
  - Limit access
  - Log access and record all specific changes
  - Require inspection and approval of changes
- ❑ A Government provided supply chain threat briefing

Values assigned for risk reduction and cost are for example. Programs must develop estimates for their environment for risk reduction and cost to implement.

Examples of Possible Design Countermeasures

Risk	Cost
-2	H
-1	M
-1	L
-2	L
-2	M
-2	M
-2	H

Possible system design countermeasures for critical functions with risk lowering impact and order of magnitude cost

- ❑ A separation kernel
  - Hardware, firmware, and/or software mechanisms whose primary function is to establish, isolate, and separate multiple partitions and to control information flow between the subjects and exported resources allocated to those partitions
- ❑ Fault detection with degraded mode recovery
- ❑ Authentication with least privilege for interfacing with critical functions
- ❑ Wrappers for COTS, legacy, and developmental software to enforce strong typing and context checking
- ❑ Wrappers for COTS, legacy, and developmental software to identify and log invalid interface parameters
- ❑ Physical and logical diversity where redundancy or additional supply chain protections are required
- ❑ An on-board monitoring function that checks for configuration integrity and unauthorized access
  - Examples include honey pots which capture information about attackers, scanners and sniffers that check for signatures of attackers, and monitoring clients which check for current patches and valid configurations

Values assigned for risk reduction and cost are for example. Programs must develop estimates for their environment for risk reduction and cost to implement.

Risk-Cost-Benefit Trade Study Exercise

- **For each critical component that requires risk reduction**
  - Determine at least two countermeasures to evaluate for each component
  - Estimate the implementation cost impacts
  - Estimate the risk reduction achieved by each countermeasure (assume that a countermeasure value of -1 reduces likelihood by one band in the risk cube)

Component	Risk Rating	Countermeasures	Cost impact	Risk reduc-tion	Residual Risk Rating

- **Determine residual risk rating for future TSN analyses**
  - Determine updated risk rating after implementation of countermeasures
  - Repeat the CA, TA, VA to support a new RA to refine this rating
  - Further countermeasures may be needed

Software Assurance (SwA) Countermeasure Methodology

Inputs:

Criticality Analysis
Potential Software Development Toolsets

JCIDS Capabilities Docs
Concept of Operations
Potential Software development processes
Potential Vulnerabilities
Preferred Concept

Identify Critical Functions that will be implemented in software.

Analyze mission impact of software component failures.
Assign Criticality Levels

Identify and prioritize potential software vulnerabilities for each critical component.

Identify applicable countermeasures that make presence or exploitation of vulnerabilities less likely.

We are here

Integral Part of SE Process

Scalable automated vulnerability analysis tools

Leverage vulnerability databases (CVE,IAVA, NVDB)

Leverage catalogs of attack patterns

Leverage existing mission assurance analysis, including flight & safety critical

Outputs:

- Tables of planned/actual SwA Countermeasures
- Plans for supporting appropriate remediation strategies in contracts / source evaluation

Completing the Software Assurance Table

Development Process Section

1. **Determine the secure design and coding standards for developmental software**
2. **Divide software into categories for the SWA Table**
3. **Decide which categories of software (development and COTS/GOTS) will need to conform to the secure design and coding standards**
4. **For the selected SW categories**
   - enter plan numbers for the "static analysis", "design inspections" and "code inspection" columns and
   - Incorporate contractor requirements into SOW
5. **Determine which categories of COTS and open source need to check vulnerabilities in CVE and enter plan numbers in the "CVE" column**
6. **Determine applicable attack patterns from CAPEC and the SWA categories that will be evaluated with respect to the attack patterns**
   - Determine as set of attack patterns for your program or require that the contractor will determine the applicable attack patterns
   - Determine the SWA categories to be evaluated with respect to the attack patterns
   - Complete the "CAPEC" column of the SWA table
7. **Use the selected attack patterns to determine the applicable weaknesses and categories of software to be evaluated with respect to those weaknesses**
   - Determine the set of applicable weaknesses or require the contractor to select the applicable weaknesses
   - Determine the SWA categories to be evaluated with respect to the weaknesses
   - Complete the "CWE" and the "Pen Test" column of the SWA table
8. **Determine test coverage**
   - Select test coverage percentage definition as percentage of SLOC branches take or function points tested
   - Work with DT&E and OT&E to identify test coverage and pen test coverage requirements by category
   - Make sure the more critical software has more test coverage (consider safety critical SW)

Completing the Software Assurance Table

Development Process Section

1. Determine the secure design and coding standards for developmental software

Either: Define a program or PEO specific set of secure design and coding standards drawing upon

- the "top 10 secure coding practices" (https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices)
- and the CWE/SANS top 25 most dangerous software errors (http://cwe.mitre.org/top25/index.html)
- and the secure design patterns (www.cert.org/archive/pdf/09tr010.pdf - 2009-10-23) to use with all Level I Mission Critical Function components.

See example on next chart

OR Add a SOW clause to have the contractor define the secure design and coding standards by SRR

- [SOWxxx?] The contractor shall develop and provide a set of secure coding standards and secure design features at the SRR.
- [SOWxxx?] The secure design and coding standard shall draw upon the "top 10 secure coding practices" (securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices) and the CWE/SANS top 25 most dangerous software errors (http://cwe.mitre.org/top25/index.html) and the secure design patterns (www.cert.org/archive/pdf/09tr010.pdf - 2009-10-23) to use with all Level I Mission Critical Function components.

In either case have the contractor define the secure design and coding standards implementation details by SRR

- [SOWxxx?] The contractor shall define the implementation level secure design and coding standards and present the secure design and coding standards at the SRR.

Consider having independent verification of conformance to the secure design and coding standards for the most critical software

- [SOWxxx?] The contractor shall employ independent verification of conformance to secure design and coding standards in accordance with the provided software assurance table

Consider making the secure design and coding standards part of the section L RFP proposal response requirements

Secure design and Coding Standards Sample Table

Type	Practice
Design	Threat Modeling
	Use Least Privilege
	Implement Sand Boxing
Secure Code	Minimize Use of Unsafe String and Buffer Functions
	Validate Input and Output to Mitigate Common Vulnerabilities
	Use Robust Integer Operations for Dynamic Memory Allocations and Array Offsets
	Use Anti-Cross Site Scripting (XSS) Libraries
	Use Canonical Data Formats
	Avoid String Concatenation for Dynamic SQL Statements
	Eliminate Weak Cryptography
	Use Logging and Tracing
Technology	Use a Current Compiler Toolset
	Use Static Analysis Tools

See - http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf

Completing the Software Assurance Table

Development Process Section

2. Divide software into categories for the SWA Table. Here are some categories to consider

- Developmental Software
  - CPI software
  - Level I critical function software
  - Level II critical function software
  - Other software
- COTS / GOTS and Open Source
  - CPI software
  - Level I critical COTS, GOTS and Open source
  - Level 2 critical COTS, GOTS and Open source
  - Divide these as necessary if there needs to be different percentages for COTS, GOTS and Open source
- Partition the code in such away that 100% can be used as the plan number for a the first 6 columns

See example on following chart

Sample Software Categories Steps 1 and 2

Development Process									
Software (Critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW								
Developmental Level I Critical Function SW								
Developmental Level II Critical Function SW								
Other Developmental SW								
COTS LVL I & II Critical Function SW								
GOTS Lvl I Critical Function SW								
Open Sources Lvl I & II Critical Function SW								
COTS (other than Critical Function) and NDI SW								

Notes:

Completing the Software Assurance Table

Development Process Section

3. **Decide which categories of software (development and COTS/GOTS) will need to conform to the secure design and coding standards**
   – The most critical should conform before the less critical
   – Conformance adds additional cost
   – Conformance increases the prevention and detection of attacks
   – Consider the Systems Categorization (MAC Level) when deciding the portions of the code that will need to conform to the secure design and coding standards

4. **For the selected SW categories**

   enter plan numbers for the "static analysis", "design inspections" and "code inspection" columns

   – The contractor can use any combination of static analysis, design inspection and code inspection to ensure conformance to secure design and coding standards

Incorporate contractor requirements into SOW

[SOWxxx?] The contractor shall ensure that static analysis, design inspections and code inspection are used to ensure conformance of applicable software categories to the secure design and coding standards. (see Defense Acquisition Guide section 13.7.3)

Sample Software Categories Steps 3 and 4

Development Process									
Software (Critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW	100/tbd	100/tbd	100/tbd					
Developmental Level I Critical Function SW	100/tbd	100/tbd	100/tbd					
Developmental Level II Critical Function SW	100/tbd	100/tbd	100/tbd					
Other Developmental SW	None/	None/	None/					
COTS LVL I & II Critical Function SW	None/	None/	None/					
GOTS Lvl I Critical Function SW	5/tbd	5/rbd	5/tbd					
Open Sources Lvl I & II Critical Function SW	5/tbd	5/tbd	5/tbd					
COTS (other than Critical Function) and NDI SW	None/	None/	None/					

Notes:

1. Contractor must update the “tbd” columns with numbers at each of the SETRs
2. The contractor can use any combination of static analysis, design inspection and code inspection to ensure conformance to secure design and coding standards for the first three columns
3. Contractor will inspect 5% of the GOTS and open source code for conformance to secure design and coding standards and recommend a remediation approach by SFR

Completing the Software Assurance Table

Development Process Section

5. **Determine which categories of COTS and open source that need to check vulnerabilities in CVE and enter plan numbers in the "CVE" column**
   - This column is not applicable to developmental software

6. **Determine applicable attack patterns from CAPEC and the SWA categories that will be evaluated with respect to the attack patterns**
   - Determine as set of attack patterns for your program or require that the contractor will determine the applicable attack patterns
   - Determine the SWA categories to be evaluated with respect to the attack patterns
   - Complete the "CAPEC" column of the SWA table
7. **Use the selected attack patterns to determine the applicable weaknesses and categories of software to be evaluated with respect to those weaknesses**
   - Determine the set of applicable weaknesses or require the contractor to select the applicable weaknesses
   - Determine the SWA categories to be evaluated with respect to the weaknesses
   - Complete the "CWE" and the "Pen Test" column of the SWA table

See example of attack vectors and associated weaknesses on next page

Selected CAPEC Attacks and Related CWE Weaknesses – Example

- ❑ CAPEC-186: Malicious Software Update
  - CWE-494: Download of Code Without Integrity Check
- ❑ CAPEC-439: Integrity Modification During Distribution
  - No related CWEs listed in CAPEC schema/taxonomy
- ❑ CAPEC-54: Probing an Application Through Targeting its Error Reporting
  - CWE-209: Information Exposure Through an Error Message
  - CWE-248: Uncaught Exception
  - CWE-717: OWASP Top Ten 2007 Cat A6 - Information Leakage & Improper Error Handling
- ❑ CAPEC-113: Application Programming Interface (API) Abuse/Misuse
  - CWE-676: Use of Potentially Dangerous Function
- ❑ CAPEC-441: Malicious Logic Inserted Into Product
  - No related CWEs listed in CAPEC schema/taxonomy
- ❑ CAPEC-10: Buffer Overflow via Environment Variables
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
  - CWE-118: Improper Access of Indexable Resource ('Range Error')
  - CWE-20: Improper Input Validation
  - 7 other related CWEs also listed in CAPEC schema/taxonomy

❑ Supply Chain Attacks

❑ Threats Mitigated by Strengthening System Design

Sample Software Categories Steps 5,6 and 7

Development Process								
Software (Critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW	100/tbd	100/tbd	100/tbd	NA	100/tbd	100/tbd	Yes	
Developmental Level I Critical Function SW	100/tbd	100/tbd	100/tbd	NA	100/tbd	100/tbd	Yes	
Developmental Level II Critical Function SW	100/tbd	100/tbd	100/tbd	NA	None/	None/	No	
Other Developmental SW	None/	None/	None/	NA	None/	None/	No	
COTS LVL I & II Critical Function SW	None/	None/	None/	100/tbd	100/tbd	100/tbd	Yes	
GOTS Lvl I Critical Function SW	5/tbd	5/rbd	5/tbd	NA	100/tbd	100/tbd	Yes	
Open Sources Lvl I & II Critical Function SW	5/tbd	5/tbd	5/tbd	100/tbd	100/tbd	100/tbd	Yes	
COTS (other than Critical Function) and NDI SW	None/	None/	None/	20/tbd	None/	None/	No	

Notes:

1. Contractor must update the "tbd" columns with numbers at each of the SETRs
2. The contractor can use any combination of static analysis, design inspection and code inspection to ensure conformance to secure design and coding standards for the first three columns
3. Contractor will inspect 5% of the GOTS and open source code for conformance to secure design and coding standards and recommend a remediation approach
4. **Contractor shall identify CVE vulnerabilities for the indicated percentage of the "other COTS and NDI" software and recommend whether the remaining "Other COTS/NDI needs to have CVE vulnerabilities identified**
5. **Contractor shall identify and present applicable attack patterns from CAPEC by category no later than SFR**
6. **Contractor shall identify and present applicable CWE weakness for the selected attack patterns along with any necessary additional abuse cases no later than SFR**
7. **The select attack vectors and weaknesses along with additional abuse cases will be used for penetration test**

Completing the Software Assurance Table

Development Process Section

8. **Determine test coverage**
   - Select test coverage percentage definition as percentage of SLOC branches take or function points tested
   - Work with DT&E and OT&E to identify test coverage and pen test coverage requirements by category
   - Make sure the more critical software has more test coverage (consider safety critical SW)

Sample Software Categories Steps 8

Development Process								
Software (Critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW	100/tbd	100/tbd	100/tbd	NA	100/tbd	100/tbd	Yes	50/tbd
Developmental Level I Critical Function SW	100/tbd	100/tbd	100/tbd	NA	100/tbd	100/tbd	Yes	60/tbd
Developmental Level II Critical Function SW	100/tbd	100/tbd	100/tbd	NA	None/	None/	No	50/tbd
Other Developmental SW	None/	None/	None/	NA	None/	None/	No	45/tbd
COTS LVL I & II Critical Function SW	None/	None/	None/	100/tbd	100/tbd	100/tbd	Yes	60/tbd
GOTS Lvl I Critical Function SW	5/tbd	5/rbd	5/tbd	NA	100/tbd	100/tbd	Yes	60/tbd
Open Sources Lvl I & II Critical Function SW	5/tbd	5/tbd	5/tbd	100/tbd	100/tbd	100/tbd	Yes	60/tbd
COTS (other than Critical Function) and NDI SW	None/	None/	None/	20/tbd	None/	None/	No	45/tbd

Notes:

1. Contractor must update the “tbd” columns with numbers at each of the SETRs
2. The contractor can use any combination of static analysis, design inspection and code inspection to ensure conformance to secure design and coding standards for the first three columns
3. Contractor will inspect 5% of the GOTS and open source code for conformance to secure design and coding standards and recommend a remediation approach
4. Contractor shall identify CVE vulnerabilities for the indicated percentage of the “other COTS and NDI” software and recommend whether the remaining “Other COTS/NDI needs to have CVE vulnerabilities identified
5. Contractor shall identify and present applicable attack patterns from CAPEC by category no later than SFR
6. Contractor shall identify and present applicable CWE weakness for the selected attack patterns along with any necessary additional abuse cases no later than SFR
7. The select attack vectors and weaknesses along with additional abuse cases will be used for penetration test
8. **Test coverage percentage is determined based upon the percentage of branches executed and based upon DT&E recommendation of at least 45% minium**

SWA Questions

A detailed SWA tutorial is available as well as additional assistance

Contact:

Tom Hurt – Thomas.D.Hurt.civ@mail.MIL 571-372-6129

Mark Cornwell – Mark.R.Cornwell2.CTR@mail.MIL 571-372-6129

–

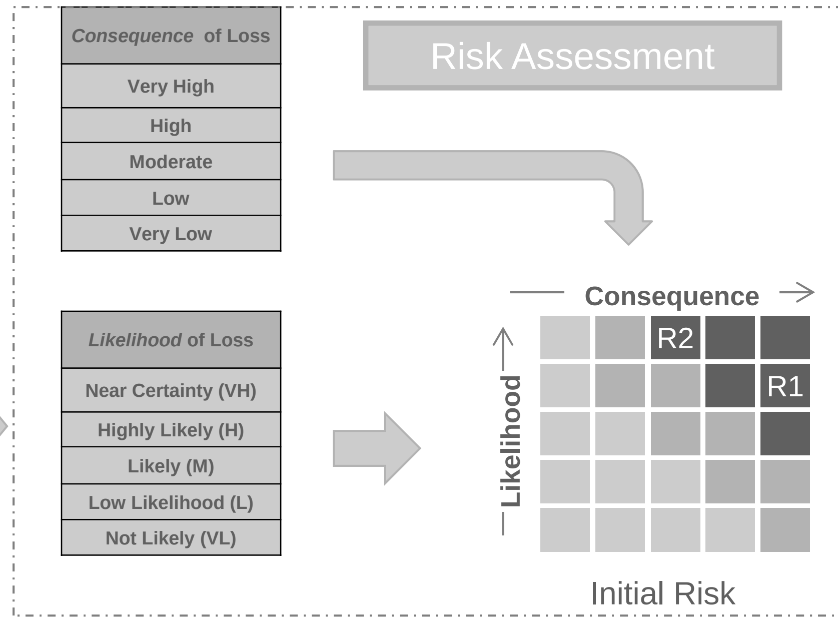
Mitigated Risk

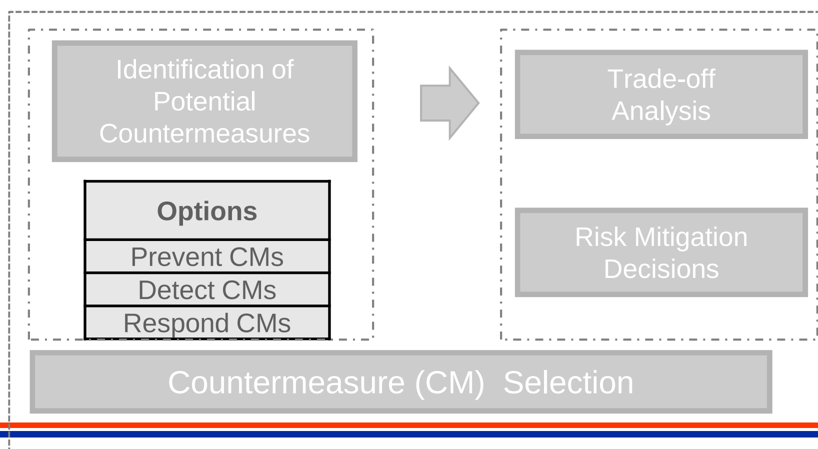
Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

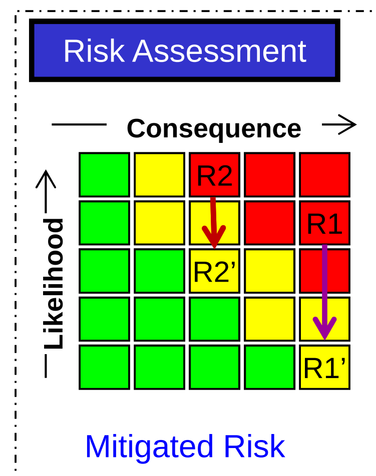
Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Critical Function	Confidentiality Vulnerability	Integrity Vulnerability	Availability Vulnerability
CF 1	High	Medium	Medium
CF 2	High	Low	Low
CF 3	Low	Medium	Medium







Other Analysis Considerations

- **Does the analysis cover the full system or just an increment or subsystem?**
- **Have the development and supply environments been considered along with the operational environment?**
- **Have protections to the development and supply processes and environments been considered along with the operational protections?**
- **Was an objective risk management method used?**
- **Did the analysis result in a comprehensive set of cyber protections for prevention, detection, and response?**
- **Has the analysis been updated as the system requirements and design are specified in more detail?**
  - The TSN analysis methodology (CA, TA, VA, RA, and CS) is a broad engineering analysis tool, applicable beyond the requirements analysis phase, across the full system development and acquisition lifecycle.

RFP Sections

RFP Package

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
- **Section C: Description/specifications/work statement**
  - **System Requirements Document (SRD - SPEC)**
  - **Statement of Work (SOW)**
  - **Contract Deliverable Requirements List (CDRLs)**
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- **Section L: Instructions, conditions, and notices to offerors**
- **Section M: Evaluation factors for award**

- **Incorporate Design Protections**
  System Requirements Document (SRD), Specification, or equivalent
- **Incorporate Process Protections**
  Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or equivalent
- **Contract Deliverable Requirements List (CDRLs)**
  Data Item Description (DID)

- **Description of program protection processes for Level I and Level II critical components**
  Sections L and M

Potential Basic Protection Requirements (1 of 4)

General Requirements for the SOW

- **The contractor shall:**
  - Perform updated TSN analyses at each of the SETRs to:
    - Identify mission critical functions and associated components and assess their criticality levels
    - Identify development and supply chain malicious insertion vulnerabilities, potential technology exploitations, and fielded system compromises
    - Utilize threat assessments
    - Identify and analyze development, design, and supply chain risks for Level I and Level II critical functions/components
    - Identify risk reduction countermeasures (mitigations) based upon a cost-benefit trade study
  - Provide and discuss TSN analysis results and the evolving security requirements and designs at each SETR
  - Maintain multi-level visibility into the supply chain of the critical function components
  - Extend these responsibilities to sub-tier suppliers of critical function components
  - Incorporate government provided intelligence

Potential Basic Protection Requirements (2 of 4)

Requirements for the Supply Chain and Development Processes/Environment

- **For Level I (and II) critical functions/components, the contractor shall implement the following basic protections (unless justified by a cost-benefit analysis):**
  - A supplier management plan that
    - Includes supplier selection criteria to reduce supply chain risks
    - Evaluates and maintains a list of suppliers and alternate suppliers with respect to the criteria established
    - Identifies functionally equivalent alternate components and sources
  - An anonymity plan that
    - Protects the baseline design, test data, and supply chain information
    - Uses blind buys for component procurement
  - Access controls that
    - Further limit access beyond normal program control
    - Log access and record all specific changes
    - Establish data collection for post attack forensic analysis
    - Require inspection and approval of changes
  - Use of secure design and coding standards
  - Black hat attack testing of the system, development environment, and supply chain
  - Red team testing
  - Material and non material attack/compromise response process development

Potential Basic Protection Requirements (3 of 4)

Potential Basic Design Requirements

- **For Level I (and II) critical functions/components, the contractor shall implement the following design protections (unless justified by a cost-benefit analysis):**
  - Least privilege implementation using distrustful decomposition (privilege reduction) or a similar approach, to move Level I critical functions into separate mutually untrusting programs*
  - Physical and logical diversification of components for critical functions which require redundancy to meet reliability or safety requirements
  - Physical and logical diversification with voting to establish trustworthiness of selected Level I critical function components
  - Wrappers for COTS, legacy, and developmental software to enforce strong typing, context checking, and other interface validation methods for interfaces with critical functions
  - Wrappers for COTS, legacy, and developmental software to identify and log invalid interface data using secure logging approaches

*See SEI -2009-TR-010

Potential Basic Protection Requirements (4 of 4)

RFP Requirements to Evaluate Each Offeror's Approach To Implementing Basic Protections

- **Section L (Instructions, conditions, and notices to offerors) should include:**
  - The contractor shall describe for Level I (and II) critical functions and components the approach to implementing basic protection processes and secure designs
  - Potential specific instructions might include:
    - Supplier management and the use of an anonymity plan
    - Maintenance of multi-level visibility into the supply chain of the critical function components
    - TSN analysis to determine and mitigate development, design, and supply chain risks
    - Establishing and use of secure design and coding standards
    - Use of secure design patterns and least privilege for critical functions
    - Use of physical and logical diversification for critical function components
- **Section M (Evaluation factors for award) should include:**
  - The above section L statements

Evaluation Criteria (1 of 9) See backup charts for complete set

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 1	**Update Record/Description/POCs**	**Outline &Guidance (O&G), Section 1**		
	Nothing beyond basic compliance			**SE**
Section 2	**Program Protection Summary**	**O&G, Section 2**		
2.1	PMO has overlaid appropriate future protection activities for their program, including, but not limited to, Critical Protection Information, Defense Exportability Features, Trusted System and Networks, Information Assurance, Vulnerability Assessments, Threat Assessments, and Countermeasure / Mitigation selection and implementation.	**O&G, Section 2.1**	**S**	**SE**
2.2a Table 2.2-1	Identified Critical Program Information (CPI) is listed	**DoDI 5200.39 Para 4.d; O&G, , Section 2.2-1**	**C**	**SE**
2.2b Table 2.2-1	Critical Functions and associated components (or potential components considered when known) are listed	**DoDI 5200.44, para 4.d, Enclosure 2, Para 8.a.(4); O&G, Section 2.2-1**	**C**	**SE**
2.2d Table 2.2-1	CPI and critical functions and components (including inherited and organic) are mapped to the security disciplines (countermeasures 1-16 from key), selected Countermeasures are accurately cross-referenced to what is documented throughout completed document.	**O&G, Section 2.2; DAG Chapters 2.3.12.2. and 13.3**	**S**	**SE**
Section 3	**CPI and Critical Components**	**O&G, Section 3**		
3.1a	CPI: Methodology for CPI is documented, to include inherited and organic CPI.. PMO has identified inherited and organic CPI as appropriate. Methodology should be repeatable, includes timing of updates to CPI, is repeatable and contains a list of functional participants. For updated PPP's, process may show additional refinement.	**O&G, Section 3.1 and 3.2**	**S**	**SE**
3.1b	Inherited and organic CPI is listed	**O&G, Section 3.1**	**S**	**SE**

Early Systems Engineering (MSA Phase) Key Points

- **It is both possible and necessary to perform meaningful system security engineering prior to Milestone A**
  - Mission critical system functions and some potential implementing components can be identified
  - Known generic attacks within the supply chain and the system/software development processes/environments, mapped against the notional system architecture, can be used to inform a vulnerability assessment to uncover exploitable weaknesses
  - A risk-based cost-benefit trade-off can be performed to select protection requirements to incorporate into the TD Phase RFP SOW and SRD
- **The SOW should indicate that further program protection analysis is a Government-Industry shared responsibility throughout the remainder of the lifecycle as the system is refined and details are determined**

Learning Objectives

- Describe the trusted systems and networks requirements analysis to address supply chain and malicious insertion threats
- Show the risk-based cost-benefit trade to select supply chain and malicious insertion countermeasures and requirements (risk mitigations)
- Describe basic supply chain and malicious insertion protections to incorporate in the early phase requirements definition and RFP
- Recognize that supply chain and malicious insertion program protections are a shared government-industry responsibility

Tutorial Thoughts

1. **What did you like most?**

2. **What most needs improvement?**

3. **What specific changes do you recommend?**

Questions?

Appendix

Evaluation Criteria (1 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 1	**Update Record/Description/POCs**	**Outline &Guidance (O&G), Section 1**		
	Nothing beyond basic compliance			**SE**
Section 2	**Program Protection Summary**	**O&G, Section 2**		
2.1	PMO has overlaid appropriate future protection activities for their program, including, but not limited to, Critical Protection Information, Defense Exportability Features, Trusted System and Networks, Information Assurance, Vulnerability Assessments, Threat Assessments, and Countermeasure / Mitigation selection and implementation.	**O&G, Section 2.1**	**S**	**SE**
2.2a Table 2.2-1	Identified Critical Program Information (CPI) is listed	**DoDI 5200.39 Para 4.d; O&G, , Section 2.2-1**	**C**	**SE**
2.2b Table 2.2-1	Critical Functions and associated components (or potential components considered when known) are listed	**DoDI 5200.44, para 4.d, Enclosure 2, Para 8.a.(4); O&G, Section 2.2-1**	**C**	**SE**
2.2d Table 2.2-1	CPI and critical functions and components (including inherited and organic) are mapped to the security disciplines (countermeasures 1-16 from key), selected Countermeasures are accurately cross-referenced to what is documented throughout completed document.	**O&G, Section 2.2; DAG Chapters 2.3.12.2. and 13.3**	**S**	**SE**
Section 3	**CPI and Critical Components**	**O&G, Section 3**		
3.1a	CPI: Methodology for CPI is documented, to include inherited and organic CPI.. PMO has identified inherited and organic CPI as appropriate. Methodology should be repeatable, includes timing of updates to CPI, is repeatable and contains a list of functional participants. For updated PPP's, process may show additional refinement.	**O&G, Section 3.1 and 3.2**	**S**	**SE**
3.1b	Inherited and organic CPI is listed	**O&G, Section 3.1**	**S**	**SE**

Evaluation Criteria (2 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 3	**CPI and Critical Components**	**O&G, Section 3**		
3.1c	Mission Criticality Analysis: Method for Criticality Analysis is documented, to include inherited and organic Critical Functions/Components. PMO has identified inherited and organic critical functions/components, as appropriate. Methodology should be repeatable, includes timing of updated to Criticality Analysis and contains a list of functional participants. and critical components, For updated PPP's, process may show additional refinement.	**O&G, Section 3.1**	**S**	**SE**
3.2 **Table 3.2-1**	Table has been completed for programs that have identified inherited Critical Functions/Components, and/or CPI, as appropriate. Cross reference with Criticality Analysis, and/or ASDB and AT Plan, as appropriate	**O&G, Section 3.2, Table 3.2-1**	**S**	**SE/ATEA**
3.3 **Table 3.3-1**	Table had been completed with program's organic Critical Functions/Components, and/or CPI, as appropriate. Cross reference with Criticality Analysis, and/or ASDB and AT Plan	**O&G, Section 3.3,** **Table 3.3-1**	**S**	**SE/ATEA**
3.3b table 3.3-1 and A_c table C-1	Expected Critical Functions and components (as identified) align with system domain acquisition, system engineering technical review expectations.	**DoDI 5200.44 section 1.a; O&G, Section 3.3**	**C**	**SE**
Section 4	**Horizontal Protection**	**O&G, Section 4**		
	PMO describes methodology that will be used to resolve issues/disagreements for horizontal protection CPI.	**O&G, Section 4**	**S**	**SE**
	For identified horizontal CPI, PMO indicates how the horizontal CPI will be protected.	**O&G, Section 4**	**S**	**SE**
	For Identified CPI Program has entered CPI into ASDB	**O&G, Section 4**	**S**	**SE**
Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**		
5.0 **Table 5.0-1**	Supply Chain Threats and Vulnerabilities to CPI and Critical Functions/Components and Countermeasures to mitigate resulting risks are included in Table 5.0.1: Summary of CPI Threat, Vulnerabilities, and Countermeasures. Supply Chain Risks are included Cross Reference with Section 5.3.4	**DoDI 5200.44 Para 4.a-e; O&G, Section 5.0;**	**S**	**CIO (SCRM/TSN)**

Evaluation Criteria (3 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**		
5.0 **Table 5.0-1**	Documents Countermeasures, including Information Assurance, that are selected to mitigate risks of compromise Cross reference with IA Strategy and 5.3.2	**O&G, Section 5.0**	**S**	**CIO (IA)**
5.1a	Threat assessments for each critical component supplier (or potential supplier) listed in Table 5.1-1: Threat Product References	**O&G, Section 5.1**	**S**	**CIO (SCRM)/SE**
5.1 **Table 5.1-1**	Defense Intelligence Agency (DIA) Threat Analysis Center (TAC) Threat Assessment Requests are developed for initial or updated Level I and selected Level II critical components based on criticality analysis (including functions that critical functions depend upon and those functions that have unmediated access to critical functions) Threat Product References; document each critical component supplier (or potential supplier) that has been assessed	**DoDI 5200.44 Para 1.d, Enclosure 2 Para 6, 8; O&G, , Section 5.1; DAG Chapter 13.4.1.2**	**C**	**CIO (SCRM)/SE**
5.1 **Table 5.1-1**	Table contains program's list of Threat Reports, as applicable	**DAG Chapter 8**	**C**	
5.1 **Table 5.1-2**	Identified Threats contained in Threat Products from Table 5.1-1 are listed in Table. Possible threats may include, but not limited to, TAC Results, other supply chain threats (receiving, transmission, transportation, …) and Information Assurance threats are listed in Table 5.1 2: Identified Threats	**5200.44 Para 1.d; O&G, Appendix E, para 5**	**C**	**SE/ CIO(IA/SCRM)**
5.1e	PMO has developed a Risk Mitigation plan for all POA&M All TAC request with a high or critical report require a documented POA&M , or risk acceptance has been documented with rationale.	**DoDI 5200.44 Para1.d and 4.a-e, Enclosure 2 Para 8; O&G Section 7**	**C**	**SE/ CIO(IA/SCRM)**
5.1f **Table 5.1-2**	If TAC results are not available, PMO has assumed a medium to medium-high supplier threat for level I critical functions	**DoDI 5200.44 Para 1.d and4.a-e; O&G Section 5.1-2**	**S**	**SE / CIO (SCRM)**
5.2a	The vulnerability determination process is described at a high level, to include methodology that program will use to identify new vulnerabilities for system and development environment, frequency this will be done and methodology to mitigate identified vulnerabilities.	**O&G Section 5.2; DAG Chapter 13.5.4**	**S**	**CIO (SCRM/IA)**
5.2b **Table 5.2-1**	For MS A, potential design, development, supply chain and malicious insertion CPI and critical function vulnerabilities are listed. For MS B,C, or FRP/FDD specific design, development, supply chain and malicious insertion CPI and critical function vulnerabilities are listed and assessed.	**DoDI 5200.39 Para4.dDoDI 5200.44 Para 1.a; O&GSection 5.2 and 5.2-1**	**C**	**SE/ CIO(SCRM)**

Evaluation Criteria (4 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**		
5.3a	Implementation of each countermeasure used to protect CPI and critical functions and components is succinctly described in each of the following 5.3 subsections. If SCRM Key Practices apply, describe which ones.	**DoDI 5200.44 Para 1.d, 4.d; O&G, Section 5.3; DAG Chapter 13.5.3**	**S**	**SE / CIO (SCRM / At / SWA/ IA / Micro)**
5.3b	PMO has described a methodology for selecting countermeasures to protect Critical Functions/Components and/or CPI, as appropriate	**O&G Section 5.3 DAG Chapter 13**	**S**	**SE**
5.3c	Countermeasures described cover prevention, detection and response	**DoDI 5200.44 para 4.c, 4.d; O&G, Section 5.3**	**S**	**SE/ CIO(SCRM)**
5.3d	Section describes the incorporation of the contract language countermeasures into the RFP statement of work, the CDRLS and the system requirements either in the main section or the applicable subsection of 5.3	**DoDI 5200.44 para 4c5,; O&G, Section 5.3**	**C**	**SE/ CIO(SCRM) / SWA / IA / AT / Micro**
5.3.1	AT POC is identified in either POC Table, Section 3.0 or 5.3.1, Plan to deliver Final AT Plan is overlaid on Program Schedule, Section 2.0, or contained in Section 5.3.1. PMO describes plan to engage with Service ATEA, as appropriate. AT Plan is submitted as an Appendix	**DoDI 5200.39 DAG Chapter 13**	**C**	**SE/ATEA**
5.3.2	POC is identified for assessing adequacy of IA Countermeasures for CPI, POC may be listed in POC Table; an Information Systems Security Engineer (ISSE) or a System Security Engineer (SSE) is identified for any program delivering Automated Information System applications.	**O&G, Section 5.3.2; DoDI 8500.2 E3.4.4**	**S**	**CIO(IA)**
5.3.2	PMO describes approach to include appropriate implementation of IA protection for contractor-owned systems hosting CPI is described	**O&G, , Section 5.3.2 DoDI 8582.01 NIST 800-53 Rev 3(or 4, if final)**	**S**	**CIO(IA)**
5.3.2	PMO describes approach for appropriate implementation of IA protection for the system being acquired is described	**O&G, Section 5.3.2**	**S**	**CIO (IA)**
5.3.3	The program establishes secure design and coding practices and/or draws on existing standards or best practices, e.g. DISA STIG, SEI "Secure Coding Standards," DHS "Build Security In,"etc..	**DoDI 5200.44 Para 4.c.(2); Guidance – generic contract language; DAG Chapter 13.6 O&G Section 5.3.3**	**C**	**SWA**

Evaluation Criteria (5 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**		
5.3.3b	PMO describes the use of Static analysis, design inspections and code inspections to inspect for the secure design and code standards established by the program, or states rationale for not implementing	**O&G Section 5.3.3; DAG Chapter 13.6**	**S**	**SWA**
5.3.3 Table 5.3.3-1	Critical function component software source code is evaluated with respect to appropriate selected [1] common weaknesses drawn from CWE or equivalent as evidenced by discussion and table summary. [should also include what is expected if PMO doesn't receive Source code]	**O&G Sec. 5.3.3, DAG Chapters 13.7.3.1.3**	**S**	**SwA**
5.3.3 Table 5.3.3-1	Critical function component COTS software (if any) is evaluated with respect to CVE, or equivalent [3], and enumerated in the table, to identify any known vulnerabilities and plans to address are described.	**DoDI 5200.44 Para 4c4; O&G Sec. 5.3.3, DAG Chapter 13.7.3.1.1**	**C**	**SwA**
5.3.3 Table 5.3.3-1	Software architectures and designs instantiating critical function components are evaluated with respect to appropriately selected attack patterns drawn from a systematic enumeration such as CAPEC as evidenced by discussion of methods employed and table percentages showing planned versus actual code evaluations.	**O&G Section 5.3.3, DAG Chapter 13.7.3.1.2**	**S**	**SwA**
5.3.3 Table 5.3.3-1	Critical function component software of unknown pedigree is protected and tested as discussed in text and/or enumerated in the table (e.g., "Operational System/Development Process" rows and "Static Analysis, Design Inspect, Code Inspect, and System Element Isolation" columns.)	**O&G, Section 5.3.3**	**S**	**SwA**
5.3.3 Table 5.3.3-1	Countermeasures are identified in the text and/or table to address how critical function component software will be protected in the operational system (e.g. table columns in "Operational Software" rows for "failover, fault isolation, least privilege, system element isolation, input checking/validation, SW Load key" countermeasures)	**O&G Section 5.3.3, Table 5.3.3-1**	**S**	**SwA**
5.3.3 Table 5.3.3-1	CWE-compatible tools are used to scan critical function component software for weaknesses and enumerated in the "Development Process" rows of the table.	**O&G Section 5.3.3 DAG Chapter 13.7.3.1.3**	S	SWA

Evaluation Criteria (6 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 5	**Threats, Vulnerabilities, and Countermeasures**	**O&G, Section 5**		
5.3.3 **Table 5.3.3-1**	Critical function component software design considers design principles to allow systems element functions to operate without interference from other elements as evidenced by enumeration in the "System Element Isolation" column in the "Operational System" rows of the table	**O&G Section 5.3.3** **DAG Chapter 13.7.3.2.4**	**S**	**SwA**
5.3.3 **Table 5.3.3-1**	Table entries, showing planned percentages, list numeric values greater than or equal to 0 and not a verbal description (e.g., "N/A", "partial," or "unknown.")	**DoDI 5200.44 Para 4c4;** **O&G Table 5.3.3.3-1**	**C**	**SwA**
5.3.4a	Describe the countermeasures employed to protect critical function COTS Hardware and hardware of unknown pedigree (i.e., from sources buried in the supply chain).	**O&G, Section 5.3.4**	**S**	**CIO (SCRM/TSN)**
5.3.4	Protection of critical functions and CPI in the development environment (e.g. in contractor possession) is described, including analysis of development process vulnerabilities and risks, plan for process and design mitigations necessary to assure the critical function software components	**O&G, Section 5.3.3;** **DAG Chapter 13.7.3.1 and 13.7.3.3**	**S**	**CIO (SCRM/TSN)** **SwA**
5.3.4c	Management of Supply Chain Risks to protect critical functions, components, and CPI is described	**DoDI 5200.44 Para 4.d;** **O&G, Section 5.3.4**	**S**	**CIO (SCRM/TSN)**
5.3.4d	Protection of sensitive information provided to, maintained at, and received from suppliers and potential suppliers is described	**DAG Chapter 13.7.4.2.3**	**S**	**CIO (SCRM/TSN)**
5.3.4	PMO describes methodology to employ defensive design and engineering protections to protect critical elements and functions by reducing unnecessary or unmediated access within system design is described	**O&G Section 5.3.4; DAG Chapter 13.7.4.2.4**	**S**	**CIO (SCRM/TSN)**
5.3.4.1	For systems employing Application Specific Integrated Circuits (ASICs) tailored or made for DoD use, section contains a plan that describes how the ASICs are either procured from a trusted supply chain comprised of suppliers accredited by DMEA, or procured utilizing a security risk assessment approach.	**DoDI 5200.44, Para 4.c.(2), 4e; CNSSD 505 Section IV, 11.;** **O&G, Section 5.3.4.1**	C	**MICRO**
5.3.4.2	Section contains description of plan (or references Counterfeit Prevention Plan) to prevent microelectronic counterfeits (of any kind) in CPI and critical components when items are not obtained from the original equipment manufacturer, original component manufacturer or from an authorized distributor.	**DoDI 5200.44 Para 1b, 4c3;** **DoDI 4140.01, Enc 4, 1.d,;** **CNSSD 505 Section IV, 10.b.2.;** **O&G, Section 5.3.4.2**	C	**MICRO**

Evaluation Criteria (7 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 8	**Foreign Involvement**	**O&G Section 8.0**		
8.0	Program summarizes international activities and any plans for foreign cooperative development. Program described how they will utilize the TS/FD Office, how export requirements will be addressed if a foreign customer/sale is identified,	**O&G Section 8.1** **DTM 11-053**	**C**	**IC**
Table 8.0-1	Table aligns with Acquisition Documents that contain Foreign Involvement activities, ie Acquisition Strategy	**O&G Table 8.0-1**	**C**	**IC**
8.1	For designated DEF Pilot Programs, PMO has included description of plan to identify, develop, and incorporate technology protection for the purpose of enhancing or enabling each system's exportability.	**O&G Section 8.1** **NDAA FY 2011, Section 254**	**C**	**IC**
Section 9	**Process for Management and Implementation of PPP**	**O&G Section 9.0**		
9.1a	Audits and Inspections are addressed	**O&G Section 9.1**	**S**	**SE**
9.1b	References to SEP PPP SETR criteria requiring updated PPP analysis before each SETR are described	**O&G Section 9.1**	**S**	**SE**
9.2a	PMO has updated the PPP for each SETR including, but not limited to, Critical Protection Information, Defense Exportability Features, Trusted System and Networks, Information Assurance, Vulnerability Assessments, Threat Assessments, and Countermeasure / Mitigation selection and implementation (including SCRM and IA).	**DoDI 5200.44 Para 4.a, 4.c,** **O&G Section 9.2** **NDAA FY 2011 Section 254** **DoDI 5200.39 DAG Chap 13**	**C**	**SE (TSN) / CIO (SCRM)**
9.3a	Countermeasures are identified and implementation plans are described addressing how supply chain and malicious insertion penetration, blue team, or red team testing are included in the verification and validation criteria, process and procedures	**DoDI 5200.44 Para 4.a, 4.c.4; O&G Section 9.3**	**C**	**SE**
9.3b	Describe how the program will integrate system security requirements testing into the overall test and evaluation strategy is described	**O&G Section 9.3**	**S**	**CIO IA**
9.4a	Program Protection during Sustainment is addressed with respect to periodic (every 12-18 months) and event driven (tech refresh, enhancement) PPP analysis and PPP updates	**O&G Section 9.4**	**S**	**SE**
9.4b	Program Protection, including but not limited to supply chain and information assurance risks, is addressed throughout the entire system lifecycle to ultimate system disposal with respect to periodic (12-18 months) and event driven (tech refresh, enhancement) PPP analysis and PPP updates. Link to the relevant Lifecycle Sustainment Plan (LCSP) language.	**O&G Section 9.4;** **DoDI 5200.44, Para 4.c;** **DAG Chapter 2.3.12.4**	**S**	**CIO (SCRM/TSN/IA)**

Evaluation Criteria (8 of 9)

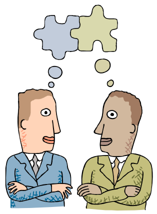
PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Section 10	**Process for Monitoring and Reporting Compromises**	**O&G Section 10.0**		
10.0a	Plan for responding to system compromise, including those resulting from supply chain, information assurance, exfiltration, compromise of CPI , is summarized.	**O&G, Section 10.0**	**S**	**SE/ CIO(SCRM/IA)**
10.0b	Supply Chain Compromise or Exploit is defined	**O&G Section 10.0**	**S**	**CIO (SCRM)**
5.3.4a	Countermeasures that protect critical function COTS Hardware, software and firmware and , hardware / software of unknown pedigree (i.e., from sources buried in the supply chain) are tested and verified	**O&G, Section 5.3.4**	**S**	**CIO (SCRM/TSN)**
Section 11	**Program Protection Costs**	**O&G Section 11.0**		
11.2	Acquisition and Systems Engineering Protection Costs Table Completed (includes SCRM and IA costs)	**O&G Section 11.2; DAG Chapters 8.4.6.7, 13.12.2**		**SE/SCRM/IA**
Appendices	**Appendices**	**O&G Mandatory Appendices**		
C.1	Criticality Analysis – updated for each PPP to reflect the updates and elaboration to the system design	**DoDI 5200.44 Para 1a; O&G Mandatory Appendices**	**C**	**SE**
C.2	Critical functions include functions which have unmediated access to the critical functions, functions critical function depend upon and defensive functions	**DoDI 5200.44, Glossary Part II ; O&G, Section 2.2-1**	**S**	**SE/ CIO (SCRM)**
C.3	An updated CA, CF and CC were completed for this version of the PPP	**DoDI 5200.44 section 1.a;O&G, Section 3.3**	**C**	**SE**
D	Critical Program Information (CPI) is assessed for criticality IAW Anti-Tamper Guidelines. The overall system AT Level is determined based on the CPI assessment.	**DoDI 5200.39 Para 4.b, 4.d; AT Guidelines, Version Table 1**	**C**	**AT**
3.1d	CPI is assessed for AT criticality with rationale for the AT criticality levels determined	**AT Guidelines, Vs2, Table 1**	**S**	**ATEA**
E.1a	Appendix E: Acquisition IA Strategy (AIAS) is included as appendix. (each PPP or as required by events)	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices;**	**C**	**CIO (IA)**

Evaluation Criteria (9 of 9)

PPP Requirements		Policy and Guidance References	Criteria	Authoritative Organization
Appendices	**Appendices**	**O&G Mandatory Appendices**		
E.1b	Appendix E: The AIAS follows the outline (or contain major outline elements), and should address appropriate guidance elements described in each section,	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices;**	**C**	**DASD C3 Cyber / CIO**
E.1c	Appendix E: The AIAS identifies MAC and CL for the system,	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices;**	**C**	**DASD C3 Cyber / CIO**
E.1d	Appendix E 2.A.2: Baseline IA Control Sets implemented for non-SCI systems agrees with table E4.T2 of DoDI 8500,2 according to MAC and CL identified.	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices;**	**C**	**DASD C3 Cyber / CIO**
E.1e	(Future pending update to DAC/O&G) Appendix E, III.1a addresses how Systems Engineering and C&A activities will be/has been integrated and incorporated into the SEP.	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices;**	**S**	**DASD C3 Cyber / CIO**
E. 1f	(Future pending update to DAG/O&G) Appendix E, II.A.4 addresses integration of Baseline IA controls, as well as any applicable JCIDS "Desired Capabilities," into the Systems Engineering requirements baselines appropriate to the lifecycle phase,	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices; DODI 8500.2 E3.4.4**	**S**	**DASD C3 Cyber / CIO**
E.1g	(Future pending update to DAG/O&G) Appendix E, II.A.4 addresses traceability of controls to elicited IA requirements, the corresponding design, and to testing.	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices; DODI 8500.2 E3.4.4**	**S**	**DASD C3 Cyber / CIO**
E.1h	(Future pending update to DAG/O&G) Appendix E, VI A. addresses integrating Developmental Test with C&A to ensure that all elicited IA requirements are tested and results leveraged to inform C&A risk management decision and documentation.	**DoDI 5200.44 Para 4d; O&G Mandatory Appendices; DODI 8500.2 E3.4.4**	**S**	**DASD C3 Cyber / CIO**

Criticality Analysis Considerations (1/2)

- **Use Mission Threads to Identify Critical Functions**
  - Based on likelihood of mission failure if the function is corrupted or disabled
  - Derived during pre-Milestone A, revised as needed for successive development milestones
- **Group Mission Capabilities by Relative Importance, As Applicable**
  - Training or reporting functions may not be as important as core mission capabilities
- **Map Critical Functions to System's Critical Components**
  - Based on likelihood of mission failure if the component is corrupted or disabled
  - Includes Critical Subsystems, Configuration Items, and Components

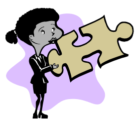


- **Map Critical Subsystems, CIs, and sub-CIs (Components) to Information and Communications Technologies (ICT's)**
  - Logic-bearing components have been singled out as often implementing critical functions and as susceptible to lifecycle corruption
- **Assign Criticality Levels to the Identified CIs or Components, Criteria May Include:**
  - Frequency of component use across mission threads
  - Presence of redundancy – triple-redundant designs can indicate critical functions.

Identifying Mission Critical Functions

Criticality Analysis Considerations (2/2)

- **Identify Any CIs or Components That Do Not Directly Implement Critical Functions, But Either Have Unmediated Communications Access (i.e., An Open Access Channel) to One or More Critical Functions or Protect a Critical Function**
  - Which components give or receive information to/from the critical components?
  - A non-critical component may communicate with a critical function in a way that exposes the critical function to attack. In some cases, the architecture may need to include defensive functions or other countermeasures to protect the critical functions



- **Identify Critical Conditions/Information Required to Initialize the System to Complete Mission-Essential Functions**
  - What information is needed to successfully execute capabilities?
  - How is this information obtained, provided, or accessed by the system?
  - How quickly must information be received to be useful?
  - Does the sequence in which the system initializes itself (power, software load, etc.) have an impact on performance?

- **Repeat Process as System is Refined or Modified**
  - Design changes may result in adding or removing specific CIs and sub-CIs from the list of critical functions and components
  - Key Decision Points: Systems Engineering Technical Reviews, Acquisition Milestone Decisions

Vulnerability Assessment Considerations (1/2)

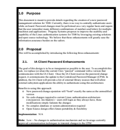
❑ Where and Under What Conditions was the System Designed?

- Who made significant system-wide design decisions?
- Who has had access to design information?
- How are requirements and specifications for critical components communicated to suppliers?
- How much do suppliers know about how critical their products are to the overall system?

❑ Where and Under What Conditions were Critical Components Developed?

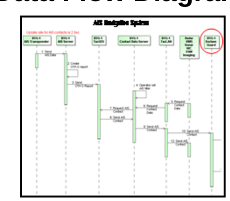
- For custom components, who made significant design decisions?
- Who has had access to design information?
- Where are critical components fabricated or manufactured?
- Who has had access to fabrication or manufacturing processes?
- What testing of critical components has been conducted? How and where?
- How are critical components shipped?
- How has custody of critical components been managed?

CONOPS



System Requirements

Data Flow Diagrams



❑ How and Where are Components Assembled and Integrated into Completed Systems?

- What final system testing is conducted?

Assessing Vulnerability of Critical Components

Vulnerability Assessment Considerations (2/2)

- **Where and under what conditions was critical software or firmware developed?**
  - How were software requirements developed and communicated?
  - Who designed the algorithms implemented in software?
  - Who designed and developed the software?
  - What design and code review or inspection processes have been employed?
  - Who has had access to the software code base? How has access to the code base been controlled?
  - What software tools (compilers, debuggers, hardware emulators, test harnesses, etc.) have been employed in developing the software?
  - What libraries of separately developed software modules have been used?
  - Are software developers able to work remotely; for example, from home?
  - How is the configuration of software and firmware managed?
  - What controls are there over the software build process?
  - How and where has the software been tested? What test criteria have been applied?

- **How are software updates distributed and loaded in the field?**
  - What verification techniques are used to ensure complete and effective updates?

- **How are other system maintenance operations conducted?**
  - How are line-replaceable subsystems managed?
  - Are depot operations established?
  - What plans are there to ensure reliable sources of replacement parts?

Tutorial Reference Catalog of Representative Attack Vectors (1 of 4)

(not exhaustive)

Attack Vector Name	Description
Reverse engineering of lost / stolen / captured components	The adversary disassembles a stolen or captured system to learn technical details about its operation and/or vulnerabilities that may be exploited
Compromise design and/or fabrication of hardware components	APT is able to compromise not merely the distribution, but the design and manufacturing of critical organization hardware at selected suppliers
Adversary intercepts hardware in distribution channel	Adversary intercepts hardware from legitimate suppliers and modifies it or replaces it with faulty hardware
Malicious software update	An attacker uses deceptive methods to cause a user or an automated process to download and install malicious code believed to be valid/authentic
Counterfeit web sites used to distribute malicious software updates	Adversary creates a duplicate of a legitimate web site, which users access and unwittingly download malicious software upgrades, patches, etc.
Components/spares no longer available	Adversaries offer necessary replacement parts, but with malware incorporated
Man-in-the-middle (MITM) supply chain	Adversary eavesdrops on sessions between organization and external supplier to gain insight into organization's supply chain needs that they can later exploit
Malicious software implantation through 3rd party bundling	The inclusion of insecure 3rd party components in a product or code-base, possibly packaging a malicious component in a product before shipping to customer.
Adversary gains unauthorized access by exploiting a software vulnerability	The adversary exploits known or unknown (0-day) software vulnerabilities to bypass security controls and gain unauthorized access
Adversary gains unauthorized access using stolen credentials	The adversary uses stolen user account information or PKI credentials to log into the system
Adversary initiates a botnet attack to disrupt network services	A botnet can be directed to spam a designated target system over a range of ports and protocols, resulting in a Distributed Denial of Service (DDoS) attack

Tutorial Reference Catalog of Representative Attack Vectors (2 of 4)

(not exhaustive)

Attack Vector Name	Description
Ex-filtration via removable media	Clandestine transfer of sensitive data to removable media, e.g., printed reports, CD, thumbdrive, etc., which is physically carried outside the security perimeter
Ex-filtration via external network	Clandestine ex-filtration of sensitive data, encrypted and transferred to a remote system outside the security perimeter using a variety of data formats
Derivation of Critical Program Information from unclassified sources	Aggregation of unclassified and/or unprotected data used to derive sensitive data
Unauthorized / unrestricted copying	Unauthorized copies of sensitive data are made and stored within the security perimeter, for future exfiltration, without document control or accountability
Clandestine changes to software or mission data	Clandestine alteration of software or data so that a system operates in a manner that compromises mission effectiveness or safety
Use of public domain info to identify and target suppliers	Suppliers are targeted for cyber and/or social engineering attack based on adversary's supply chain awareness
Netflow data used to identify critical internal workflows	Adversary analyzes netflow traffic data to identify and target key network workflows, IT resources, and/or personnel
Shell company established to export critical technologies	Adversary sets up a dummy company for the purpose of acquiring products that contain restricted or export-controlled technologies for shipment overseas
Software defects hidden/obscured by code complexity	Highly complex code can obscure software defects, even by static source code analysis tools
Use of counterfeit parts of foreign or unknown origin	Insertion of counterfeit parts of foreign origin into products destined for the U.S. having potential to degrade or sabotage performance and reliability of systems
Hardware/Software baseline manipulations	An adversary in the employ of a solution provider subverts computers and networks through subtle hardware or software manipulations

Tutorial Reference Catalog of Representative Attack Vectors (3 of 4)

(not exhaustive)

Attack Vector Name	Description
Hiding backdoors and features for unauthorized remote access	An adversary in the employ of a software supplier deliberately hides backdoors and features for unauthorized remote access and use
Foreign hardware incorporated into computing environment	Hardware incorporated into the computing environment that was manufactured overseas or acquired from a foreign-owned domestically controlled company
Foreign software incorporated into computing environment	Software incorporated into the computing environment that was developed overseas or acquired from a foreign-owned domestically controlled company
Malicious code pre-installed	Malicious code (e.g., viruses, logic bombs, self-modifying code, spyware, trojans) is pre-installed on components being integrated into the computing environment
Disruption of critical product or service	Failure or disruption in the production or distribution of a critical product or service
Malicious or unqualified service provider	Reliance upon a malicious or unqualified service-provider for the performance of technical services
Installation of unintentional vulnerabilities	Installation of hardware or software that contains unintentional vulnerabilities
Zero-day vulnerabilities	Vulnerabilities exist in new or updated software, including operating systems, for which patches or fixes do not yet exist
Misconfigured filesystem access	Discretionary access for users to system and user folders and files has been set in a manner inconsistent with access/permissions policies and intent
Compromised network server	A compromised server is used to attack client systems requesting network services, execution environments, or access to data
E-mail attachment	Means by which malicious code can be introduced into a system and potentially be capable of system compromise including data exfiltration

Tutorial Reference Catalog of Representative Attack Vectors (4 of 4)

(not exhaustive)

Attack Vector Name	Description
Password misuse	Password sharing, a form of password misuse, can lead to unaccountability with respect to execution of software based critical mission functions
Data or information leakage	Social networking sites are used by attackers to gather sensitive information about an organization, its employees, work programs, and technologies used
Auditing circumvention	Preventing a system administrator from starting an audit process could allow an adversary to carry out an attack without possible indicators being recorded
DNS spoofing (cache poisoning)	Results in rerouting a request for a web page, causing the name server to return an incorrect IP address, diverting traffic to another computer, often the attacker's
Use of open source software	Introduction of malicious code into software through insertion of malicious code into open source libraries
Malicious code insertion: Software development – *requirements analysis phase*	Hidden in software's requirements
Malicious code insertion: Software development – *design phase*	Hidden in software's design
Malicious code insertion: Software development – *implementation phase*	Appended to legitimate software code Added to linked library functions Added to installation programs, plug-ins, device drivers, or other support programs Integrated into development tools (e.g., compiler generates malicious code)
Malicious code insertion: Software development – *testing phase*	Inserted via tools during system test

DoD Terminology Reference

- **AoA Analysis of Alternatives**
- **APB Acquisition program Baseline**
- **ASR Alternative Systems Review**
- **CARD Cost Analysis requirements Description**
- **CCE Component Cost Estimate**
- **CDD Capability Development Document**
- **CONOPs Concept of Operations**
- **CPI Critical Program Information**
- **DT&E Developmental Test and Evaluation**
- **EMD Engineering and Manufacturing Development**
- **IA Information Assurance**
- **IAS Information Assurance Strategy**
- **ICD Initial Capability Document**
- **OT&E Operational Test and Evaluation**
- **LRIP Low Rate Initial Production**
- **MSA Materiel Solution Analysis**
- **PPP Program Protection Plan**
- **PRR Production Readiness Review**

- SEP Systems Engineering Plan
- RFP Request for Proposals
- SAP Security Assessment Plan
- SAR Security Assessment Report
- SP Security Plan
- SOW Statement of work
- SRD System requirements Document
- SVR/FCA Systems Verification Review/Functional Configuration Audit
- TDS Technology Development Strategy
- TEMP Test and Evaluation Master Plan
- TRR Test Readiness Review
- TSN Trusted Systems and Networks