Program Protection Implementation Considerations

Melinda Reed

Deputy Director for Program Protection

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

NDIA Program Protection Summit - Workshop

May 21, 2014

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

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, and/or degrade system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences:***
  - Loss of critical data and technology
  - System corruption
  - Loss of confidence in critical warfighting capability; mission impact

Today's acquisition environment drives the increased emphasis

Networked systems
Software-intensive
Prime Integrator, hundreds of suppliers
Advanced technology and critical components

Figure 3. Model 1: Hardware Intensive Program

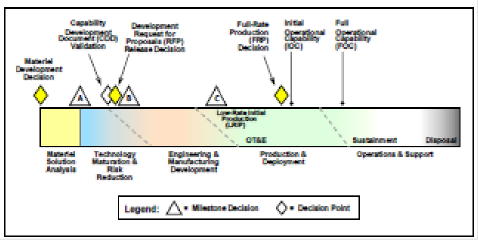

Materiel Development Decision
Capability Development Document (CDD) Validation
Development Request for Proposals (RFP) Release Decision
Full-Rate Production (FRP) Decision
Initial Operational Capability (IOC)
Full Operational Capability (FOC)
A
B
C
Low-Rate Initial Production (LRIP)
OT&E
Sustainment
Disposal
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
Legend: = Milestone Decision = Decision Point

Figure 5. Model 3: Incrementally Fielded Software Intensive Program

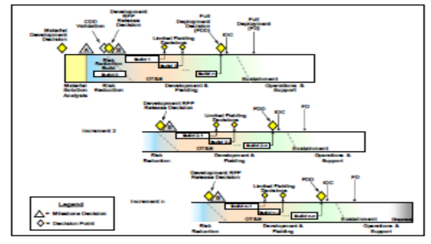


Figure 4. Model 2: Defense Unique Software Intensive Program

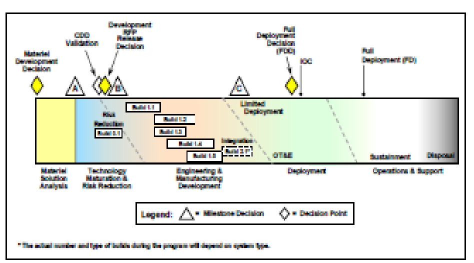
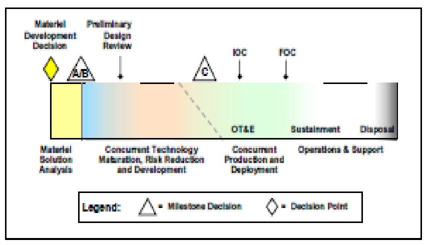
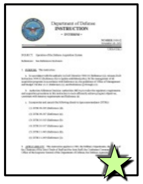


Figure 6. Model 4: Accelerated Acquisition Program

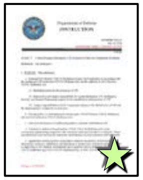

Materiel Development Decision
Preliminary Design Review
A/B
C
IOC
FOC
OT&E
Sustainment
Disposal
Materiel Solution Analysis
Concurrent Technology Maturation, Risk Reduction and Development
Concurrent Production and Deployment
Operations & Support
Legend: = Milestone Decision = Decision Point

Program Protection Integrated into Policy



Interim DoDI 5000.02 Operation of the Defense Acquisition System

– Regulatory requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD



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

– Assigns responsibility for Counterintelligence, Security, and System Engineering support for the identification and protection of CPI

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 vulnerabilities in system design or subversion of mission critical functions or components (including software, microelectronics)

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 8500.01 Cybersecurity

– Establishes a DoD cybersecurity program to protect and defend DoD information and information technology

★ - Update in process

DFARS Clause 252.204-7012: Safeguarding Unclassified Controlled Technical Information*

- **Published November 18, 2013**
  - Clause affects all new contracts that contain, or will contain unclassified controlled technical information
  - Includes flow down to all subcontracts
- **Purpose: Establish minimum requirements for DoD unclassified controlled technical information on contractor information systems**
  - Requires contractors implement minimum set of information security controls
    - 51 information security controls from NIST SP 800-53, Revision 4
    - Combination of Technical, Process, Awareness, and Training measures
  - Requires contractors report cyber incident and compromises
  - Requires contractor actions to support DoD damage assessment as needed
- **Incident Reporting**
  - Reporting includes:
    - DoD contracts and subcontractor information affected by a cyber incident or compromise
    - DoD programs, platforms, or systems involved
    - Description of DoD technical information compromised
  - Reported information does not include signatures or other threat actor indicators
- **Procedures, Guidance, and Information (PGI) in development**

*http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

Guidance and Education

- **Defense Acquisition Guidebook (DAG) is being updated to reflect Interim DoDI 5000.02 content**
  - Program Protection, Chapter 13, incorporates DAG Chapter 4 (Systems Engineering) framework, DoDI 5200.44, DoDI 8500.01, and advancements in methodology
  - *Reorganization:* Aligns with Systems Engineering framework to increase integration of Program Protection activities into DoD systems engineering
  - *Focus on overarching processes:*
    - Processes and security specialties written for PMs and systems engineers to better understand how to incorporate program protection into programs
    - Detailed guidance is transitioning to white papers that will be available on the DASD(SE) website; facilitates domain unique tailoring

- **DoD 5200.39 Manual**
  - Development effort kicked off April 2014

- **Defense Acquisition University**
  - Initiated discussions with DAU to begin building curriculum
  - Plans to develop a 100-level course and a 200-level course for PMs and SEs

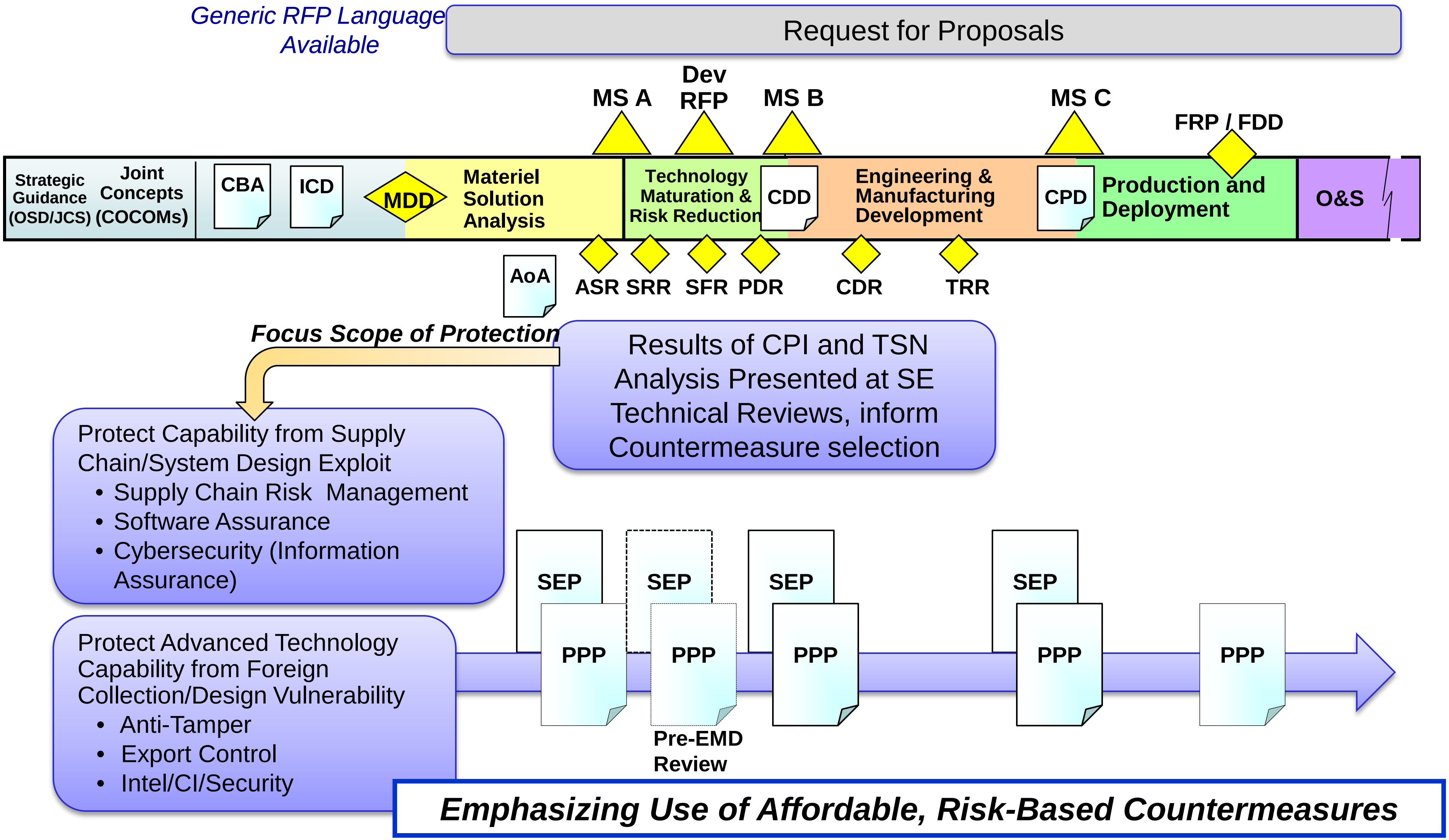
DASD(SE) Program Protection Website

- **DASD(SE) has added a Program Protection and System Security Engineering initiatives page to its website**
- **Contains the latest available policy, guidance, professional papers/presentations, and acquisition regulations for SSE**
  - Guidance available will continue to grow as more techniques for implementing PP/SSE are developed
  - Contains links to relevant Industry collaboration initiatives, including the NDIA SSE Committee
- **Recently added guidance**
  - Program Protection Plan Evaluation Criteria, Version 1.1
  - Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals
  - Software Assurance Countermeasures in Program Protection Planning

PP/SSE Initiative page is available at
http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

PPP Development and Updates



Generic RFP Language Available

Request for Proposals

MS A

Dev RFP

MS B

MS C

FRP / FDD

Strategic Guidance (OSD/JCS)

Joint Concepts (COCOMs)

CBA

ICD

MDD

Materiel Solution Analysis

AoA

Technology Maturation & Risk Reduction

CDD

Engineering & Manufacturing Development

CPD

Production and Deployment

O&S

ASR SRR SFR PDR CDR TRR

Focus Scope of Protection

Results of CPI and TSN Analysis Presented at SE Technical Reviews, inform Countermeasure selection

Protect Capability from Supply Chain/System Design Exploit
- Supply Chain Risk Management
- Software Assurance
- Cybersecurity (Information Assurance)

Protect Advanced Technology Capability from Foreign Collection/Design Vulnerability
- Anti-Tamper
- Export Control
- Intel/CI/Security

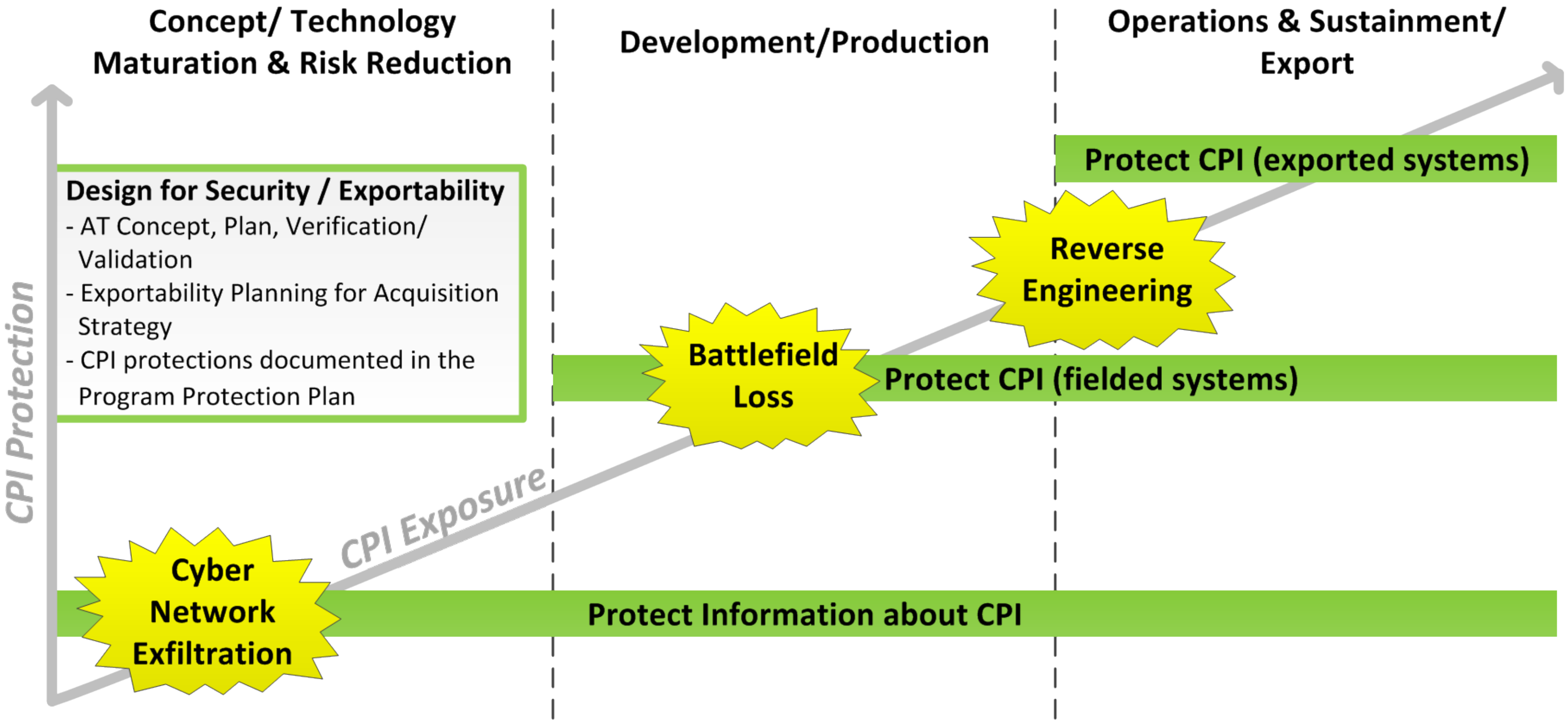
SEP SEP SEP SEP

PPP PPP PPP PPP PPP

Pre-EMD Review

Emphasizing Use of Affordable, Risk-Based Countermeasures

CPI Protection Throughout the Life Cycle

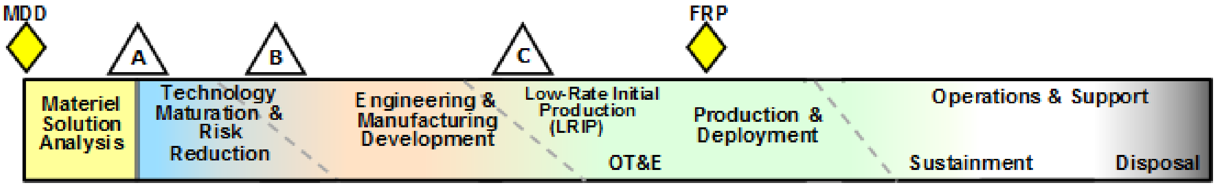

Concept/ Technology Maturation & Risk Reduction
Development/Production
Operations & Sustainment/ Export
CPI Protection
CPI Exposure
Design for Security / Exportability
- AT Concept, Plan, Verification/ Validation
- Exportability Planning for Acquisition Strategy
- CPI protections documented in the Program Protection Plan
Protect CPI (exported systems)
Reverse Engineering
Battlefield Loss
Protect CPI (fielded systems)
Cyber Network Exfiltration
Protect Information about CPI

Balance CPI exposure — threat — consequence of loss

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

Critical Program Information (CPI) Analysis Process

	Determine:	Consider:
Determine CPI	The advanced technologies to be protected	• Intelligence on foreign capabilities • Information that will derive the capability requiring protection
Assess CPI	The level of protection required based on the assessed CPI risk.	• CPI criticality • System exposure • Threat(s)
Protect CPI	The required protections / countermeasures.	• Anti-Tamper • Exportability Features • Security
Monitor CPI	The CPI that no longer requires protection. The new technologies requiring protection.	• CPI compromise and loss • Technological advantage • Emerging technologies


MDD
A
B
C
FRP
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Low-Rate Initial Production (LRIP)
OT&E
Production & Deployment
Operations & Support
Sustainment
Disposal

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

Integrating SSE into RFPs

- DASD/SE PPP Website contains a document with potential SOW and Section L SSE language

- SOW example

  The contractor shall plan for and implement countermeasures that mitigate the risk of foreign intelligence or foreign influence, technology exploitation, supply chain and battlefield threats, and vulnerabilities that result in Level I and Level II protection failures of the system;

- Section L example

  The offeror, as part of its technical proposal, shall describe the use of its system security engineering (SSE) process in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.

- DFARS Clause 252.204-7012: Safeguarding Unclassified Controlled Technical Information is also being included in contracts, subcontracts and solicitations

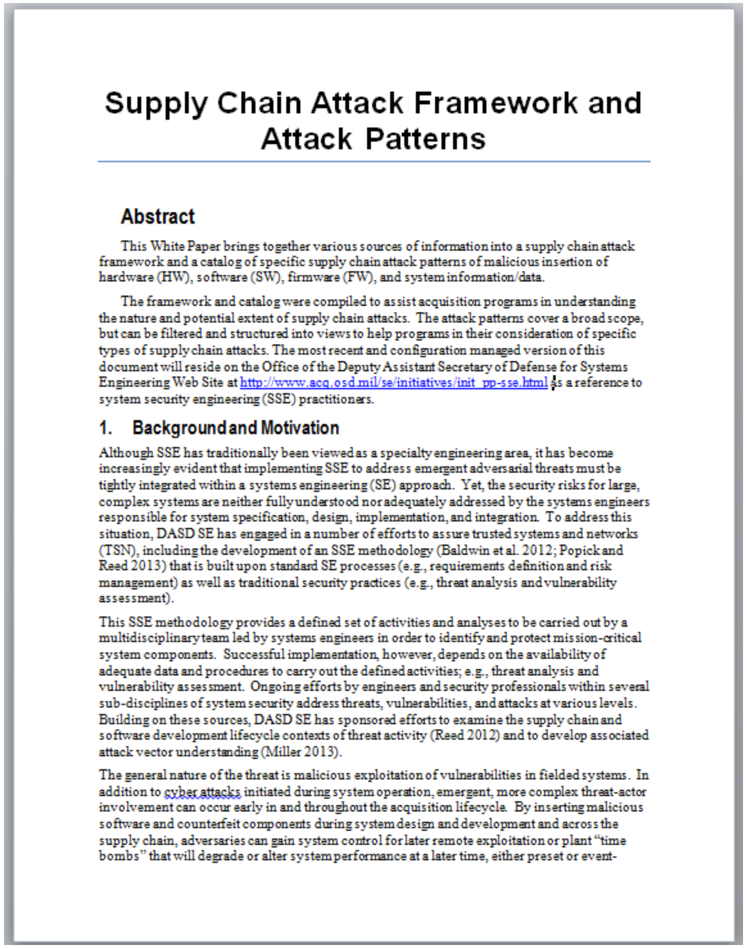
SSE Performance Metrics

SSE performance metrics are needed to assess the health of the system security implementation

- Needs to align with SE and PM performance metrics
- Provide a common set of SSE metrics to measure progress
- NDIA Study that kick-offs at the breakout sessions will focus on SSE metrics

Supply Chain Attack Framework and Attack Patterns

- OSD sponsored effort to investigate supply chain attacks and develop a framework for defining supply chain attack
- White paper available at http://www.acq.osd.mil/se/initiatives/init_pp-sse.html
- Need industry and government input to enhance the database
- Send feedback to glenda.n.turner.ctr.@mail.mil



Supply Chain Attack Framework and Attack Patterns

Abstract

This White Paper brings together various sources of information into a supply chain attack framework and a catalog of specific supply chain attack patterns of malicious insertion of hardware (HW), software (SW), firmware (FW), and system information/data.

The framework and catalog were compiled to assist acquisition programs in understanding the nature and potential extent of supply chain attacks. The attack patterns cover a broad scope, but can be filtered and structured into views to help programs in their consideration of specific types of supply chain attacks. The most recent and configuration managed version of this document will reside on the Office of the Deputy Assistant Secretary of Defense for Systems Engineering Web Site at http://www.acq.osd.mil/se/initiatives/init_pp-sse.html as a reference to system security engineering (SSE) practitioners.

1. Background and Motivation

Although SSE has traditionally been viewed as a specialty engineering area, it has become increasingly evident that implementing SSE to address emergent adversarial threats must be tightly integrated within a systems engineering (SE) approach. Yet, the security risks for large, complex systems are neither fully understood nor adequately addressed by the systems engineers responsible for system specification, design, implementation, and integration. To address this situation, DASD SE has engaged in a number of efforts to assure trusted systems and networks (TSN), including the development of an SSE methodology (Baldwin et al. 2012; Popick and Reed 2013) that is built upon standard SE processes (e.g., requirements definition and risk management) as well as traditional security practices (e.g., threat analysis and vulnerability assessment).

This SSE methodology provides a defined set of activities and analyses to be carried out by a multidisciplinary team led by systems engineers in order to identify and protect mission-critical system components. Successful implementation, however, depends on the availability of adequate data and procedures to carry out the defined activities; e.g., threat analysis and vulnerability assessment. Ongoing efforts by engineers and security professionals within several sub-disciplines of system security address threats, vulnerabilities, and attacks at various levels. Building on these sources, DASD SE has sponsored efforts to examine the supply chain and software development lifecycle contexts of threat activity (Reed 2012) and to develop associated attack vector understanding (Miller 2013).

The general nature of the threat is malicious exploitation of vulnerabilities in fielded systems. In addition to cyber attacks initiated during system operation, emergent, more complex threat-actor involvement can occur early in and throughout the acquisition lifecycle. By inserting malicious software and counterfeit components during system design and development and across the supply chain, adversaries can gain system control for later remote exploitation or plant "time bombs" that will degrade or alter system performance at a later time, either preset or event-

* The information on slides 12-16 taken from: Miller, John F, *Supply Chain Attack Framework and Attack Patterns*, MTR 140021, Dec 2013.
Case number 13-3315. Used with permission, The MITRE Corporation.

Supply Chain Attacks and Countermeasures – Catalog Attributes

Attack Catalog

- *Attack ID* *(unique ID number)*
- *Attack Point* *(supply chain location or linkage)*
- *Phase Targeted* *(acquisition lifecycle phase)*
- *Attack Type* *(malicious insertion of SW, HW, etc.)*
- *Attack Act* *(the "what")*
- *Attack Vector* *(the "how")*
- *Attack Origin* *(the "who")*
- *Attack Goal* *(the "why")*
- *Attack Impact* *(consequence if successful)*
- *References* *(sources of information)*
- *Threat* *(adversarial event directed at supply chain)*
- *Vulnerabilities* *(exploitable weaknesses)*
- *Applicable Countermeasures* *(mapped IDs)*

Mapping to Countermeasures Catalog

Countermeasures Catalog

- *CM ID*
- *CM Name*
- *CM Type*
- *CM Focus*
- *Mitigation Approach*
- *CM Description*
- *CM Goal*
- *Earliest Implementation Phase*
- *Timeframe to Implement*
- *Resources Needed*
- *Cost to Implement*
- *Amount of Risk Reduction*
- *References*
- *Implementation Action*
- *Applicable Attacks*

Points to File with Implementation Guidance

Mapping to Attack Catalog

Supply Chain Attack Vector Description Format

Attack Origin
Staff within the software engineering environment

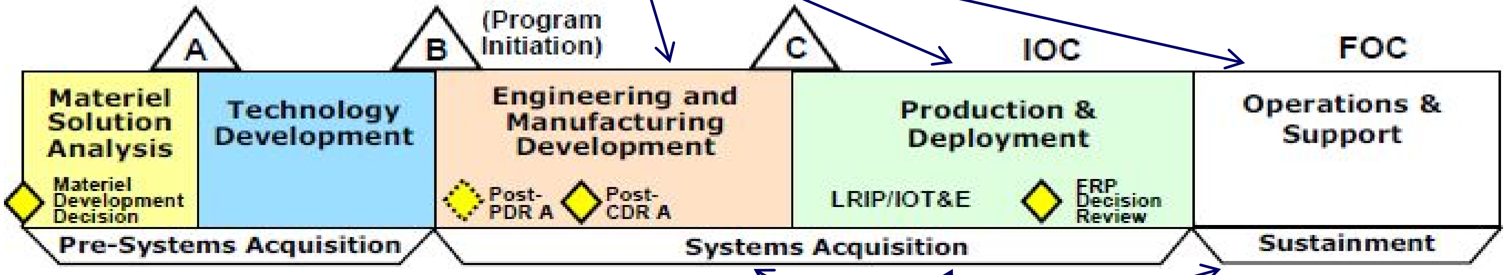
Attack Vector
Adversary with access to software processes and tools within the development environment or software support activity update environment

Attack Act
System is compromised by the insertion of malicious software into components during development or update

Attack Point
At a software developer /contractor location

Attack Type
Malicious insertion of software

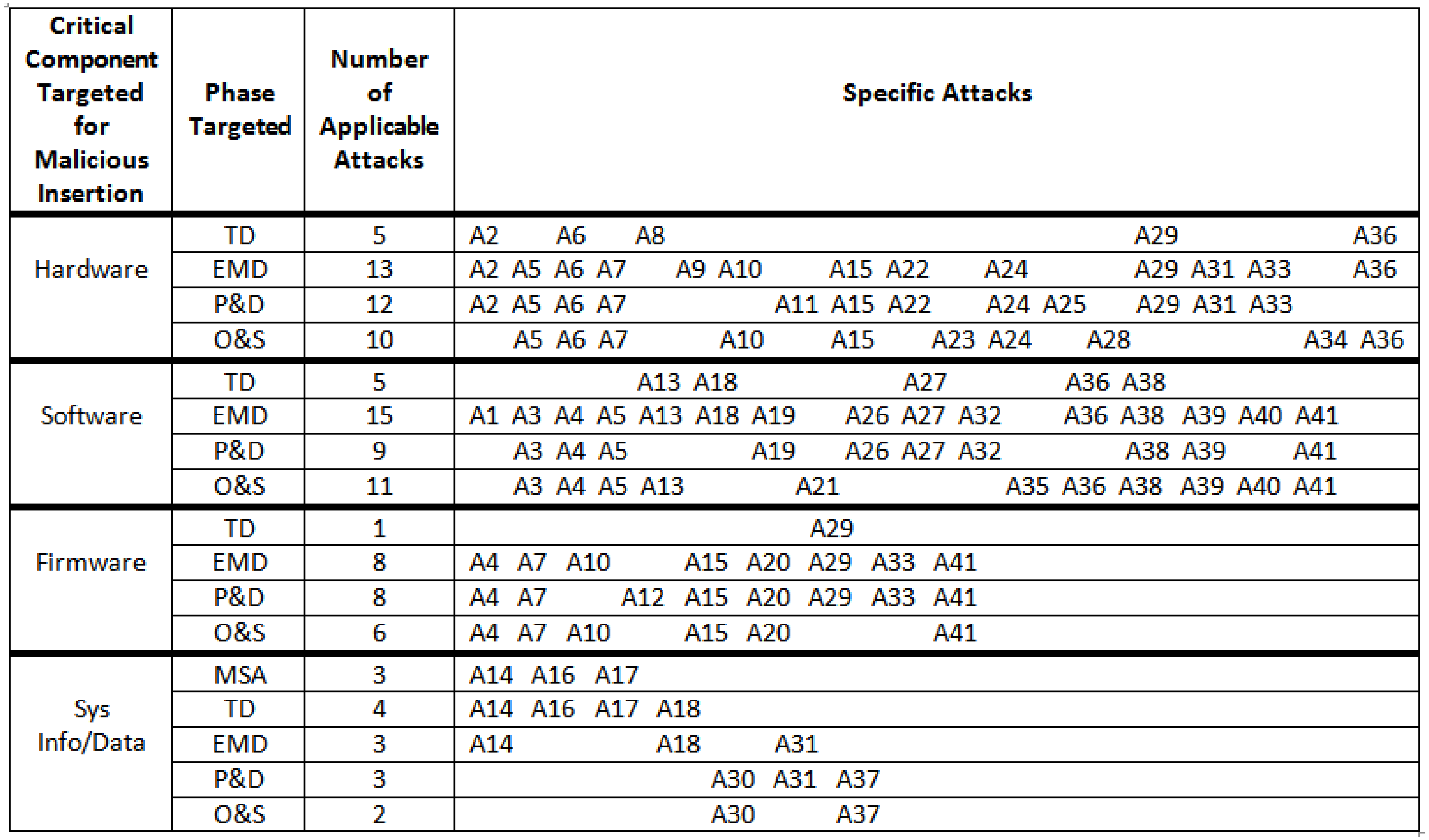
Attack Impact
System functions in an unintended manner



Phases Targeted

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

Summary of Attack Patterns By Component



Critical Component Targeted for Malicious Insertion	Phase Targeted	Number of Applicable Attacks	Specific Attacks
Hardware	TD	5	A2 A6 A8 A29 A36
	EMD	13	A2 A5 A6 A7 A9 A10 A15 A22 A24 A29 A31 A33 A36
	P&D	12	A2 A5 A6 A7 A11 A15 A22 A24 A25 A29 A31 A33
	O&S	10	A5 A6 A7 A10 A15 A23 A24 A28 A34 A36
Software	TD	5	A13 A18 A27 A36 A38
	EMD	15	A1 A3 A4 A5 A13 A18 A19 A26 A27 A32 A36 A38 A39 A40 A41
	P&D	9	A3 A4 A5 A19 A26 A27 A32 A38 A39 A41
	O&S	11	A3 A4 A5 A13 A21 A35 A36 A38 A39 A40 A41
Firmware	TD	1	A29
	EMD	8	A4 A7 A10 A15 A20 A29 A33 A41
	P&D	8	A4 A7 A12 A15 A20 A29 A33 A41
	O&S	6	A4 A7 A10 A15 A20 A41
Sys Info/Data	MSA	3	A14 A16 A17
	TD	4	A14 A16 A17 A18
	EMD	3	A14 A18 A31
	P&D	3	A30 A31 A37
	O&S	2	A30 A37

By phase:	MSA	TD (now TMRR)	EMD	P&D	O&S
Attacks	3	12	28	24	22

Example from Supply Chain Attack Database (Attack ID: A3)

Attack ID	Attack Point	Phase Targeted (Selected = Bold)	Attack Type (Selected = Bold)
A3	P2-P5	MSA TD **EMD** **P&D** **O&S**	Malicious Insertion of: - Hardware - **Software** - Firmware - Sys Info/Data

**From: Miller, John F, *Supply Chain Attack Framework and Attack Patterns*, MTR 140021, Dec 2013

Attack ID	Attack Act	Attack Vector	Attack Origin	Attack Goal (Selected = Bold)	Attack Impact	Reference
A3	System is compromised by the insertion of malicious software into components during development or update.	Adversary with access to software processes and tools within the development environment or software support activity update environment.	Staff within the software engineering environment.	**Disruption** **Corruption** **Disclosure** Destruction	System may function in a manner that is unintended.	Based on NIST SP 800-30; page E-4

Attack ID	Threat	Vulnerabilities
A3	An adversary with access to software processes and tools within the development or software support environment can insert malicious software into components during development or update/maintenance.	The development environment or software support activity environment is susceptible to an adversary inserting malicious software into components during development or update.

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

Our Focus on SSE and SE

- **DoD has policy in place for risk-based cost benefit trade-offs to protect systems, supply chains, and software development**

- **DoD is emphasizing the SSE integration with systems engineering and its contribution to the system design through:**
  - Integration of PPP into System Engineering technical reviews
  - Incorporation of program protection and SSE requirements and processes into engineering development contracts
  - Inclusion of system security risk assessments into overall Program assessment

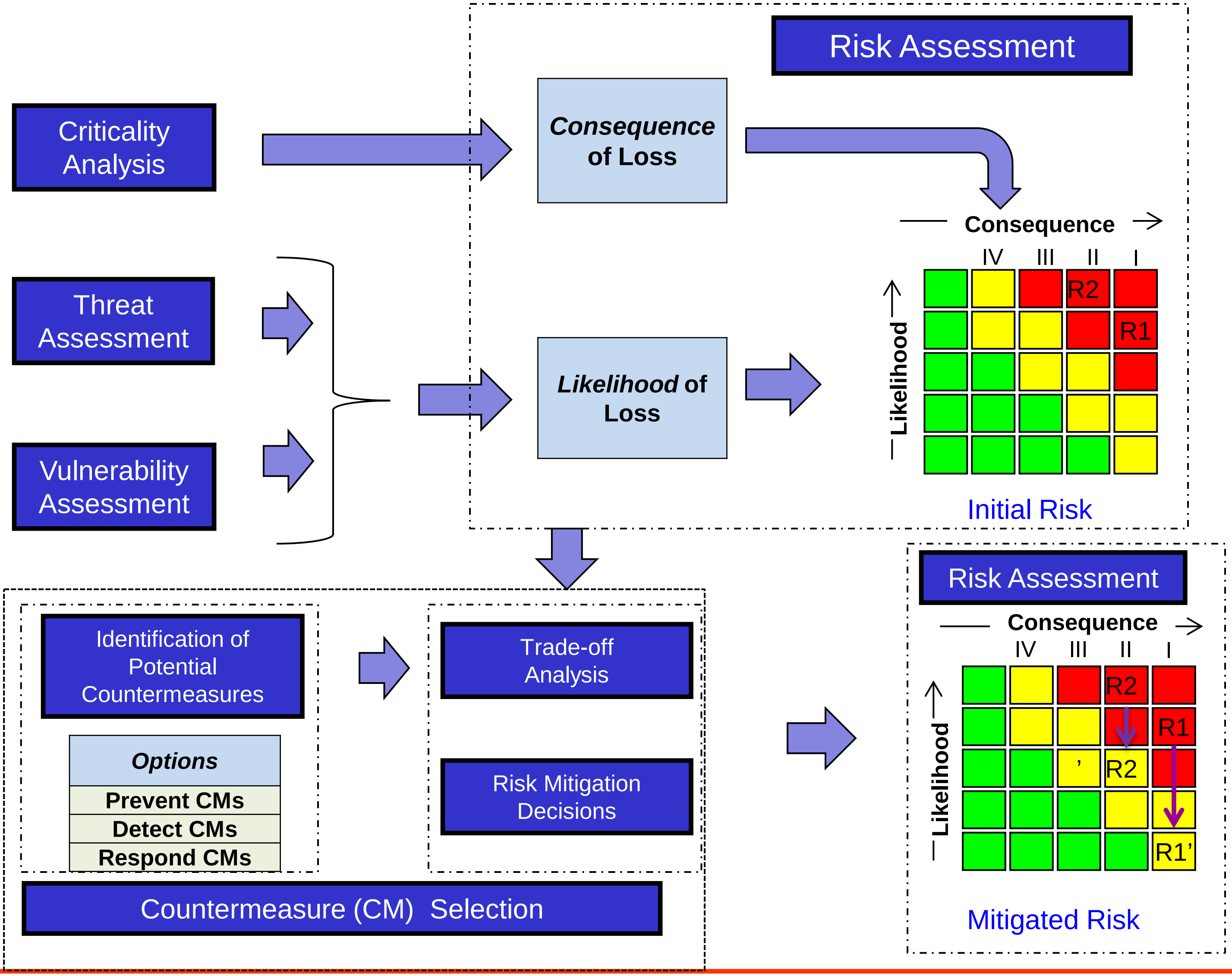
- **Industry is playing an important role in the DoD SSE initiative**

DoD efforts are emphasizing integration of system security engineering into system engineering processes and analysis throughout the system life cycle

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

Questions?

TSN Methodology



Criticality Analysis

Threat Assessment

Vulnerability Assessment

Risk Assessment

Consequence of Loss

Likelihood of Loss

Consequence →

Likelihood →

	IV	III	II	I
🟩	🟨	🟥	🟥 R2	🟥
🟩	🟨	🟨	🟥	🟥 R1
🟩	🟩	🟨	🟨	🟥
🟩	🟩	🟩	🟨	🟨
🟩	🟩	🟩	🟩	🟨

Initial Risk

Identification of Potential Countermeasures

Options
Prevent CMs
Detect CMs
Respond CMs

Trade-off Analysis

Risk Mitigation Decisions

Countermeasure (CM) Selection

Risk Assessment

Consequence →

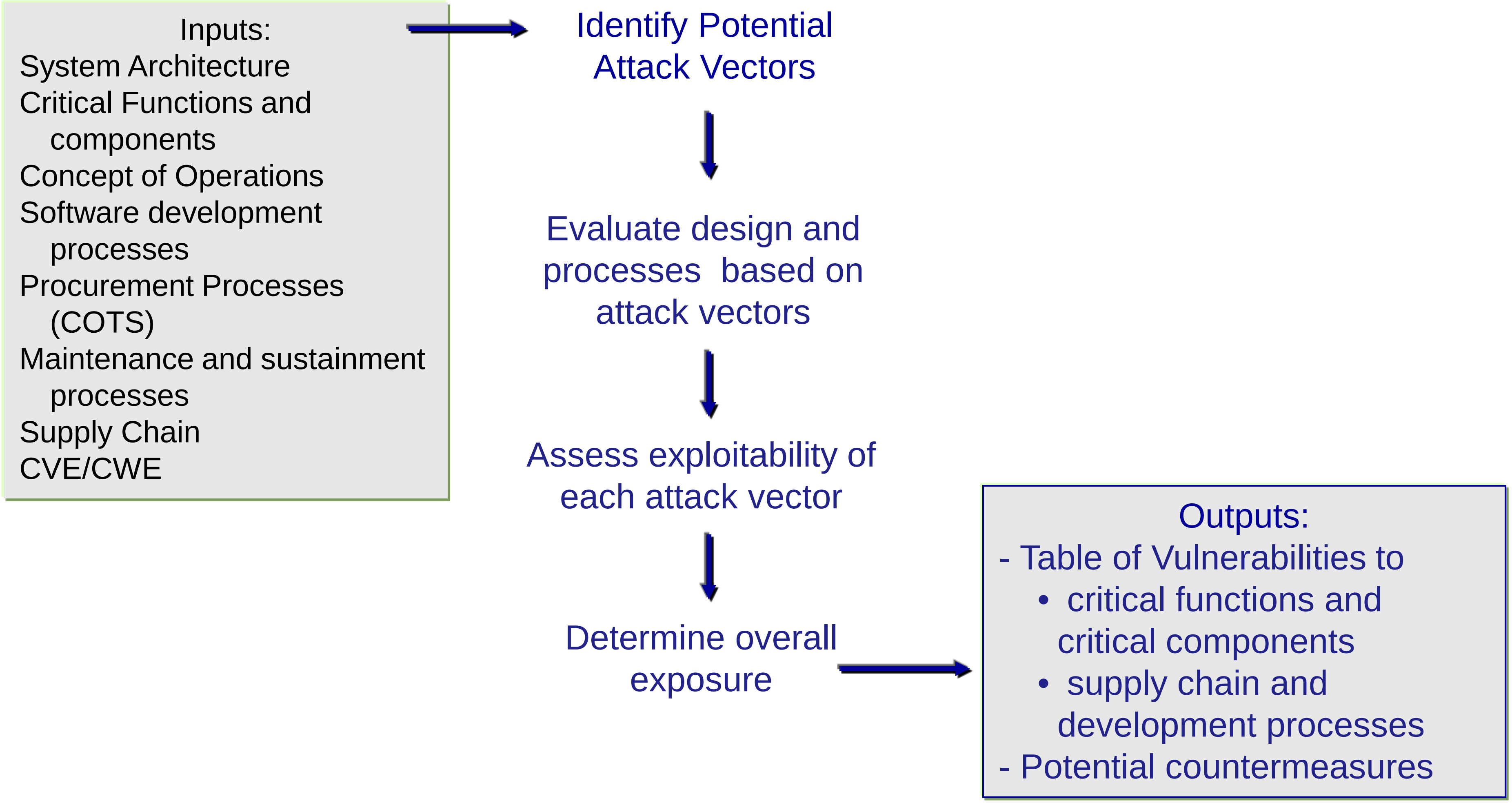
Likelihood →

	IV	III	II	I
🟩	🟨	🟥	🟥 R2	🟥
🟩	🟨	🟨	🟥	🟥 R1
🟩	🟩	🟨 ’	🟨 R2	🟥
🟩	🟩	🟩	🟨	🟨
🟩	🟩	🟩	🟩	🟨 R1’

Mitigated Risk

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.

Vulnerability Assessment



Inputs:

System Architecture

Critical Functions and components

Concept of Operations

Software development processes

Procurement Processes (COTS)

Maintenance and sustainment processes

Supply Chain

CVE/CWE

Identify Potential Attack Vectors

Evaluate design and processes based on attack vectors

Assess exploitability of each attack vector

Determine overall exposure

Outputs:

- Table of Vulnerabilities to
  - critical functions and critical components
  - supply chain and development processes
- Potential countermeasures

DoDI 5230.24
Technical Information Definition

- **The term includes technical data or computer software of any kind that can be used, or adapted for use, in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or materiel; or any technology that advances the state of the art, or establishes a new art, in an area of significant military applicability in the United States.**
  - The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.
  - Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited.