Developmental & Cybersecurity Evaluation Framework

Dr. Suzanne Beers & Peter Christensen

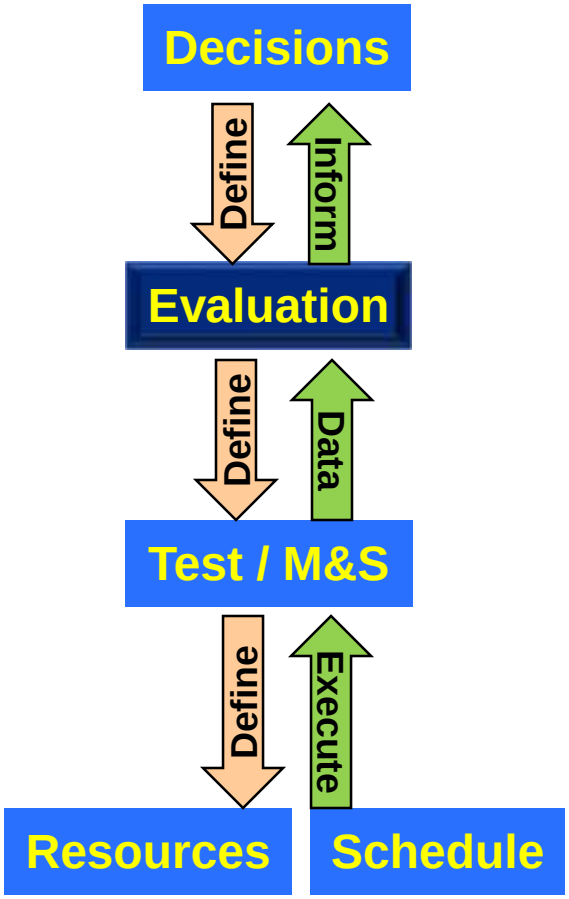
The MITRE Corporation supporting DASD(DT&E)

31st Annual International Test and Evaluation Symposium:
T&E to Achieve Better Buying Power 2.0

7 October 2014

Briefing Purpose & Overview

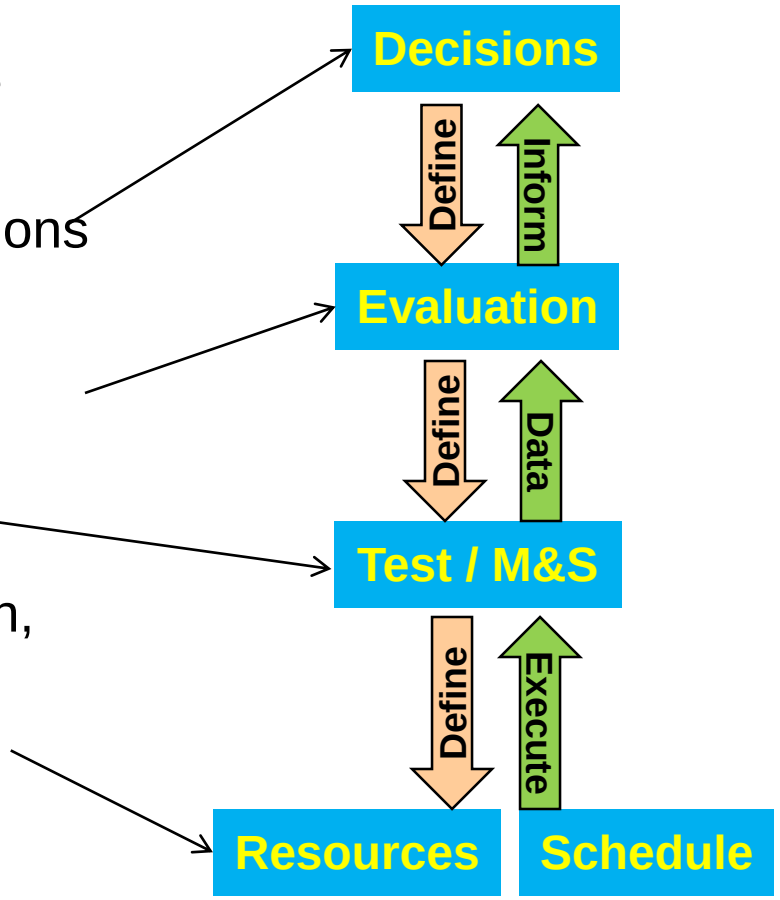
- **Developmental Evaluation Framework (DEF) part of TEMP's SE-V story:**
  - **How acquisition, technical and programmatic *decisions* will be informed by evaluation**
  - **How system will be *evaluated***
  - **How *test and M&S events* will provide data for evaluation**
  - **What *resources* are required to execute test, conduct evaluation, and inform decisions**
- **Cyber Evaluation Framework guides programs through forest of cyber/IA guidance**
  - **System/software assurance**
  - **Risk Management Framework**
  - **Vulnerability Assessment**
  - **Interoperability**



DT&E Strategy Overview

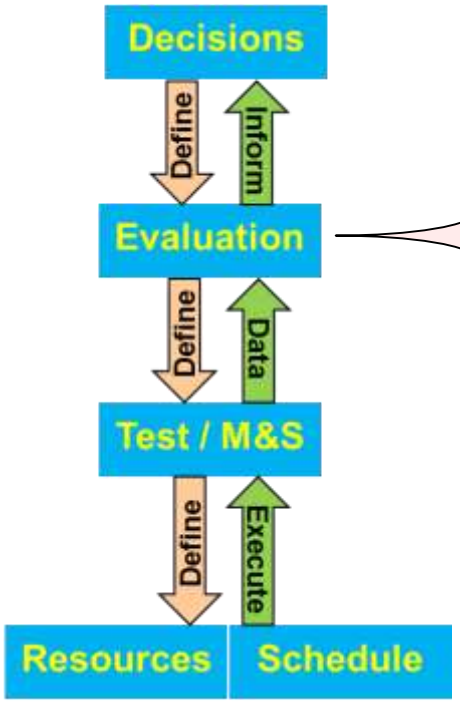
Articulate a logical *evaluation* strategy that informs decisions

- How acquisition, programmatic, technical and operational decisions will be *informed* by evaluation
- How system will be *evaluated*
- How test and M&S events will provide *data* for evaluation
- What *resources* are required to execute test, conduct evaluation, and inform decisions



DT&E story thread: decision – evaluation– test & resources

Developmental Evaluation Framework (DEF)



Capability questions

Decision Support Questions (DSQ)

System capabilities

DEO 1

DEO 2

DEO 3

Technical measures

TM 1

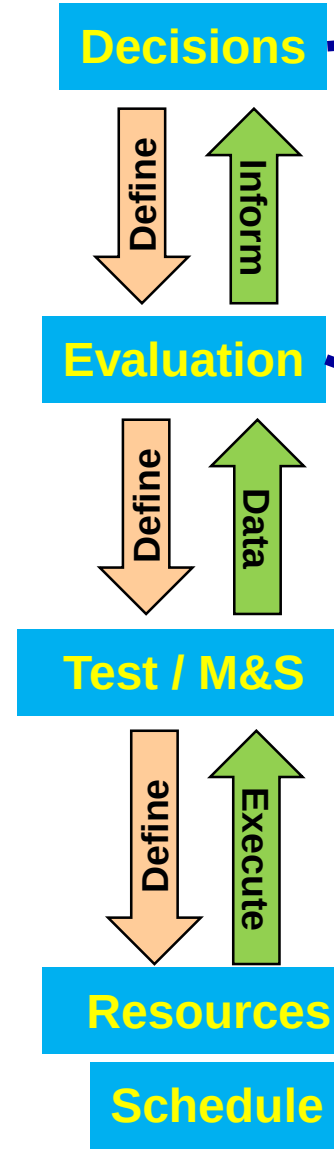
TM 2

*TM 3

KPP/KSA/CTP - related

System Engineering decomposition:
Evaluate system capability - Inform decisions

Developmental Evaluation Framework



Developmental Evaluation Objectives	System Requirements and T&E Measures		Decisions Supported							
			Decision #1		Decision #2			Decision #3	Decision #4	
			DSQ #1	DSQ #2	DSQ #3	DSQ #4	DSQ #5	DSQ #6	DSQ #7	DSQ #8
Functional evaluation areas System capability categories	Technical Reqmts Document Reference	Description	Identify major decision points for which testing and evaluation phases, activity and events will provide decision supporting information. Cells contain description of data source to be used for evaluation information, for example: 1) Test event or phase (e.g. CDT1....) 2) M&S event or scenario 3) Description of data needed to support decision 4) Other logical data source description							
Performance										
Performance Capability #1	3.x.x.5	Technical Measure #1	DT#1		M&S#2				DT#4	M&S#2
	3.x.x.6	Technical Measure #2	M&S#1		DT#3				DT#4	M&S#2
Performance Capability #2	3.x.x.7	Technical Measure #3				DT#3			IT#1	
	3.x.x.8	Technical Measure #4				M&S#4			IT#1	
Interoperability										
Interoperability Capability #3	3.x.x.1	Technical Measure #1				DT#3		DT#4		
	3.x.x.2	Technical Measure #2		IT#2		M&S#4		DT#4		
Interoperability	3.x.x.3	Technical Measure #3		IT#2				IT#1		M&S#2
	3.x.x.4	Technical Measure #4						IT#1		DT#3
Cybersecurity										
SW/System Assurance	PPP 3.x.x	SW Assurance Measure #1			SW Dev Assess		SW Dev Asses	SW Dev Assess		
RMF		RMF Contol Measure #1	Cont Assess		Cont Assess	Cont Assess	Cont Assess			
Vulnerability Assess		Vul Assess Measure #1				Blue Team			Blue Team	
Interop/Exploitable Vuln.		Vul Assess Measure #2				Red Team			Red Team	
Reliability										
Reliability Cap #1	4.x.x.1	Technical Measure #11		M-demo#1						IT#5
	4.x.x.2	Technical Measure #12		M-demo#1				IT#2		IT#5
	4.x.x.3	Technical Measure #13				M-demo#2		IT#2		
Reliability Cap #2	4.x.x.4	Technical Measure #14				M-demo#2		IT#2		

Example – Army Integrated Air & Missile Defense (AIAMD)

Sensors, weapons, mission command (MC), and communication networks for the Army Air Defense Artillery (ADA) Future Force

AIAMD DEF

Decisions

Functional Integration (3.0.2)

Functional Integration (3.1)

MS-C
(Capabilities demonstrated or on track)

Ready for IOT&E
(Capabilities demonstrated)

DSQ 1. Ready to integrate?
DSQ 2. Capability performing to include/exclude?
DSQ 3. Capability sufficient for intended use for next phase?

Capabilities	Paragraph	Measures	DSQ1
Performance:			
3.2.2 Integration	3.2.2.2.1	Geodetic Registration	
	3.2.2.2.2	Sensor Control	
	3.2.2.2.3	Common Tactical Air Picture	
	3.2.2.2.4	Estimate Launch and Impact Point Prediction	
	3.2.2.2.5	Track Capacity	
	3.2.2.2.6	Saturation Alleviation	
	3.2.2.2.7	Single Integrated Air Picture / Early Warning	
	3.2.4.7	Span of Control	
3.2.1 Employment	3.2.1.2	Task Force Tailorability	
	3.2.1.5	Modes of Control	
Interoperability:			
3.3.1 External System Interface	3.3.1.1	Joint External System Interfaces	
	3.3.1.2	Army Force External System Interfaces	
3.13.1 Network			
3.13.2 Distributed Track Manag			
Cybersecurity			
System/SW Assurance			
Risk Management Framework			
Vulnerability Assessment			
NR-KPP			
Reliability			
3.8 System Quality Factors	3.8.1	Reliability	
	3.8.2	Maintainability	
3.6 Environmental Conditions	3.6.1	Natural Environments	
	3.6.2	Induced Environments	
	3.6.3	Nuclear Biological Chemical (NBC)	
	3.6.4	Electromagnetic Environments	
3.9 Design & Construction Constraints	3.9.1	Transportability & Mobility	
	3.9.4	E3	

DEO/Capabilities

System specification capabilities (3.2.x)

Decision Support Questions

DSQ#1: Ready to integrate?

DSQ#2: Capability performing to include/exclude in SW build?

DSQ #3 Capability sufficient for intended use for next phase?

Requirements/Technical Measures

System Specification sub-capabilities
(mix of 3.2.x.x and 3.2.x.x.x to capture capability description at TEMP level of detail)

Test events / Data sources

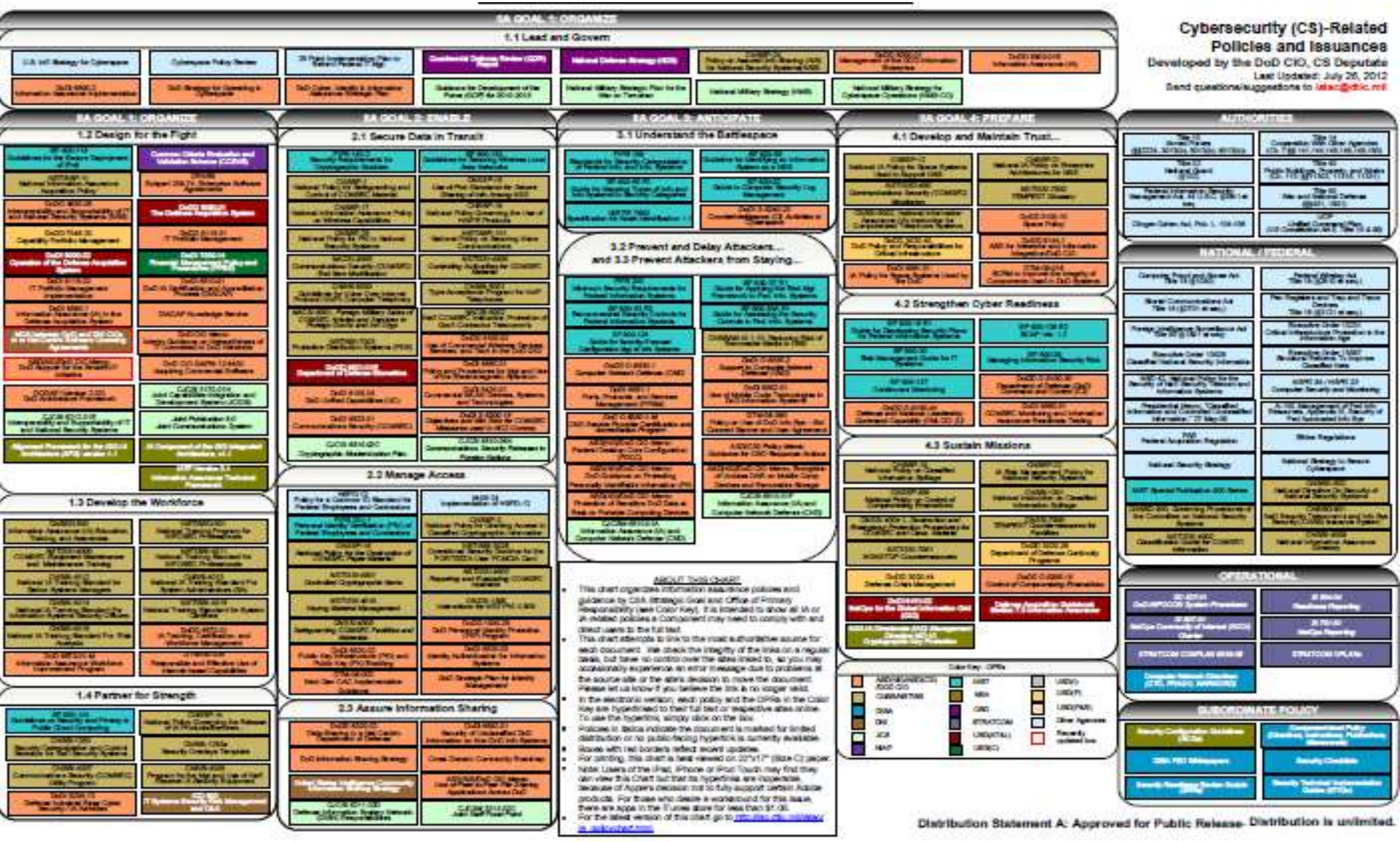
CT: Contractor Test

IV: Integration Event

SHWIL: SW/HW in the Loop

Range: Range/Flight Test

IA Policy Guidance "Shock & Awe"



Cybersecurity (CS)-Related Policies and Issuances

Developed by the DoD CIO, CS Deputate

Last Updated: July 26, 2012

Send questions/suggestions to ialac@dtic.mil

Cyber EF Roadmap Guides T&E Path

Cyber EF Roadmap Use

Cyber Technical Capability Evaluation Activity Categories	DT Objectives - Cyber Technical Capabilities	Is the system and software developed securely?	Does the system satisfy baseline Cybersecurity/IA technical standards?	Do exposed vulnerabilities adversely effect system resiliency?	Is the system sufficiently interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?	Test Activity / Data Source
Systems and Software Assurance	Software Vulnerabilities Eliminated in critical components	Program Protection Plan(PPP) Table S.3.3.-1 (example measures: number/category of SDRs, CVEs eliminated, CWEs remaining, CAPECs mitigated)				Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E
	Anti-Tamper Protections Implemented	Appendix D: Anti-tamper plan				Anti-Tamper Implementation Plan/Report
	Supply Chain Risks Mitigated	PPP Section S.3.4				Supply Chain Risk Management Report
(DIACAP) DOD IS&D/RMF C&A Requirements	Access Controls Audit and Accountability Configuration Management Continuity Enclave Boundary Defense Enclave and Computing Environment Identification and Authentication Vulnerability and Incident Management Maintenance Media Protection Personnel, Awareness, and Training Physical and Environmental (as applicable)		Measure sources includes: Cyber security Acq strat, security controls assessment plan (example measures include: X of controls verified, number/category of outstanding deficiencies)			ST&E/ Security Controls Assessed/ ACAs/ Step 3 vulnerability assessment team
	Include other "attack surfaces" as based on Step 2 analysis		Include technical standards appropriate for the attack surface, e.g. MIL-STD 461 and 464 for EMI/EMC in the intended E3 environment			Contractor T&E and government technical standard testing as appropriate
Cyber Kill Chain Vulnerability Assessment	Operational scenarios and critical missions should be based on authoritative sources including CONOPS and capabilities documents. Representative cyber threats should be developed based upon STARs and cyber attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source. Cyber kill chain as exercised by the adversary includes the following steps: Reconnaissance, Weaponization, Delivery, Exploit, Control, Execute, Maintain. Cyber Defense in response to adversarial actions include actions to redirect, obviate, impede, detect, limit, and expose adversarial actions. The lexicon reference is Intended Effects of Cyber Resiliency Techniques on Adversary Activities			ITT will develop measures. Interoperability metrics and measures should be derived from the NR-KPP. Metrics include: - Support to military operations - Enter and be managed in the network - Exchange information - Support [illegible] military operations. Sources for cyber security metrics and measures may be derived from program technical documentation, or other authoritative sources including the DoD Strategy for Operating in Cyberspace and Resilient Military Systems and Threat Defense Science Board Task Force. The below measures are derived from NIST SP 800-160, Vol 1, Cyber Resiliency Metrics, dated Apr 2012. Example metrics include: - X cyber resources properly configured - # attempted intrusions stopped at network perimeter/ deflected to honeypot - X mission-essential capabilities for which multiple instantiations available - Length of time between initial disruption and restoration - Quality of restored data - Quality of choices made during design and engineering that affect resiliency - X mission-essential datasets for which all items effectively have two or more independent external data feeds - X mission-essential data stores for which a master copy exists - X data value assertions in a mission-essential data store for which a master copy exists - Length of time between initial disruption and restoration	Step 3 Vulnerability Assessment: Team has full knowledge and access to the System and all supporting components (Blue Team)
System interoperability and functionality in response to exploited cyber vulnerabilities						Step 4 Vulnerability Assessment: Team [illegible] on adversary without knowledge or access to the [illegible] (Red Team)

Cyber EF Roadmap guides program-specific tailoring

- Categories of cyber evaluation
  - System/SW assurance
  - Compliance (C&A, RMF)
  - Vulnerability assessment (Red team, Blue team)
  - Interoperability (NR-KPP)
- Cyber capabilities within each category
- Source documents, examples of measures
- Test activities, data sources

System & Software Assurance Risk Management Framework

Overarching Developmental Issue	***Does the system satisfy the specified and derived cybersecurity technical requirements for confidentiality, availability, and integrity; and is the system able to sustain critical mission tasks in a cyber-contested environment?***	
Issue 1, Systems and Software Assurance	Are the system and the software developed securely?	
DT objectives evaluate: • Software vulnerabilities have been eliminated in critical components (source: CVE, CWE, Common Attack Pattern Enumeration and Classification) • Secure software development processes • Secure software development environment • Anti-tamper protections implemented • Supply chain risks mitigated	Measures Sources: • Software Development Plan • PPP Table 5.3.3.1 (example measures: number/category of SDRs, CVEs eliminated, CWEs remaining • Information Assurance Strategy or equivalent • PPP Appendix D: Anti-tamper plan • Supply chain risk addressed in PPP Section 5.3.4, in RFP and contracts	Test Activity/Data Sources: • Contractor T&E/ Functional Qualification Testing/ Government ST&E • Anti-tamper Implementation Plan/Report • Supply Chain Risk Management Report
Issue 2, RMF Requirements	Does the system satisfy baseline cybersecurity technical standards?	
DT objectives evaluate: • Identified attack surfaces	Measures Sources: • SAP, DoDI 8510.01, NIST Special Publication 800-53/53A, CNSSI 1253, and cybersecurity acquisition strategy (example measures include percentage of controls verified, number/category of outstanding deficiencies) • Include technical standards appropriate for the attack surface	Test Activity/Data Sources: • ST&E/ Security Controls Assessor/ ACAs/ vulnerability assessment team • Contractor T&E and government technical standard testing as appropriate

Vulnerability Assessment

Issue 3, Vulnerability Assessment	Do exposed vulnerabilities adversely affect system resiliency?	

Operational scenarios and critical missions should be based on authoritative sources, including CONOPS and capabilities documents. Representative cyber threats should be developed based upon STARs and cyber-attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source. Cyber kill chain as exercised by the adversary includes the following steps: reconnaissance, weaponization, delivery, exploit, control, execute, maintain. Cyber defense in response to adversarial actions includes actions to redirect, obviate, impede, detect, limit, and expose adversarial actions. The lexicon reference is Intended Effects of Cyber Resiliency Techniques on Adversary Activities.
 	
DT objectives evaluate:
• System and supporting networks resilience and ability to disrupt the cybersecurity kill chain
  ○ Deny and disrupt attacks
  ○ Degrade attacks
  ○ Deceive attacks
• Capability to:
  ○ Detect exploitations
  ○ Recover from system degradation
	Measures Sources:
	Interoperability metrics and measures should be derived from the NR-Key Performance Parameter (KPP). Measures include:
	• Support military operations
	• Enter and be managed in the network
	• Exchange information
	• Support net-centric military operations.
	Cybersecurity metrics and measures may be derived from program technical documentation, or other sources (e.g., the DoD Strategy for Operating in Cyberspace and Resilient Military Systems Cyber Threat Defense Science Board Task Force). The measures below are derived from MP 120053, Rev. 1, *Cyber Resiliency Metrics*, dated Apr 2012. Example metrics include:
	• Percentage of cyber resources properly configured
	• Number of attempted intrusions stopped at network perimeter/deflected to honeypot
	• Percentage of mission-essential capabilities for which multiple instantiations are available
	• Length of time between initial disruption and restoration
	• Quality of restored data
	• Quality of choices made during design and engineering that affect resiliency
	• Length of time between initial disruption and restoration.
		Test Activity/Data Sources:
		• Assessment: Blue Team has full knowledge and access to the system and all supporting components.

Interoperability & Exploited Cyber Vulnerabilities

Issue 4, System interoperability and functionality in response to exploited cyber vulnerabilities	Is the system sufficiently interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?	
DT objectives evaluate: • Entry and management on a network • Secure exchange of information • Support for net-centric military operations • Response to exploited cyber vulnerabilities • Support for military operations in a cyber-contested environment.	Measures Sources: • Interoperability measures derived from capabilities documents, Information Support Plan, integrated architectures, Technical Standards (CJCSI 6212.01F) • Cybersecurity measures and scope of Red Team testing will be based on cyber evaluation measures developed during all prior phases, to potentially include threat portrayals and penetration testing.	Test Activity/Data Sources: • Assessment: Red Team functions as an adversary without knowledge or access to the system.

Core Teams: Applying Evaluation Framework to Programs

- ***DEF*** Core Team
  - Small, focused group of T&E and program acquisition SMEs
    - Chief Developmental Tester, acquisition strategy SME, requirements SME
  - Develop DEF by facilitated discussion
    - Decision support questions (DSQ) – T&E generated knowledge needed to inform decisions
    - Developmental Evaluation Objectives (DEO) – system capabilities
    - Technical Measures (TM) – "inch deep-mile wide" quantification of capabilities

- ***Cyber EF*** Core Team
  - Small, focused group of T&E, program cybersecurity SMEs
    - Chief Developmental Tester, cybersecurity SME, requirements SME
  - Tailor generic Cyber EF roadmap to program specifics
    - Draw metrics from PPP, Anti Tamper (ATP) and Supply Chain Risk Management (SCRM) Plans, Risk Management Framework (RMF)

Summary & Way Ahead

- DEF focuses system evaluation (in mission context) to inform decisions
- Cyber EF guides cybersecurity evaluation

- Way Ahead
  - DASD(DT&E) is ready, willing, able, and anxious to help your program succeed!
  - Contact us for your DEF and/or Cyber EF Core Team