Developmental & Cybersecurity Evaluation Framework

Dr. Suzanne Beers & Peter Christensen

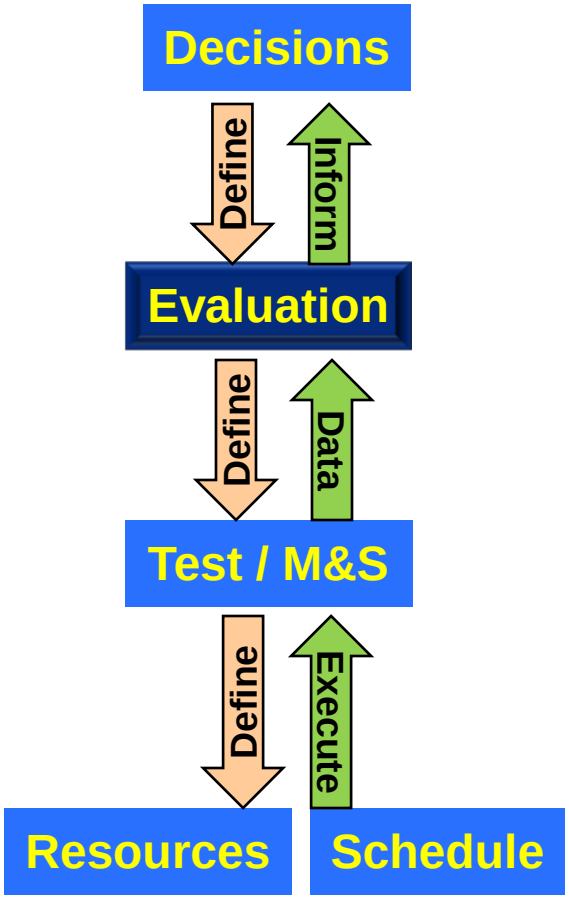
The MITRE Corporation, supporting DASD(DT&E)

NDIA T&E Conference

22-23 July 2014

Briefing Purpose & Overview

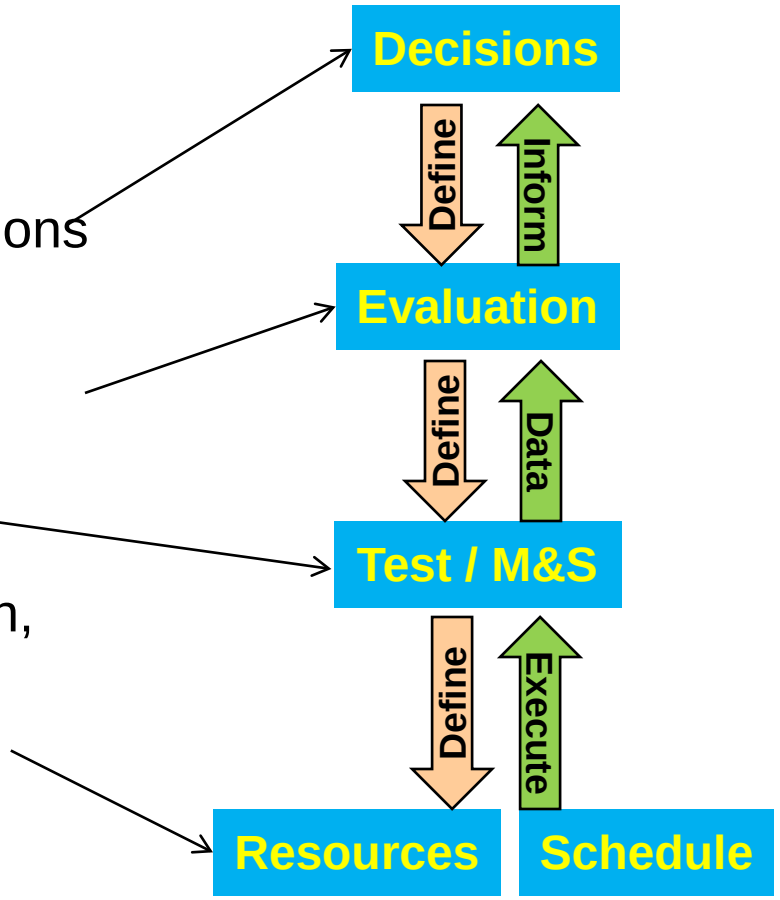
- **Developmental Evaluation Framework (DEF) part of TEMP's SE-V story:**
  - **How acquisition, technical and programmatic *decisions* will be informed by evaluation**
  - **How system will be *evaluated***
  - **How *test and M&S events* will provide data for evaluation**
  - **What *resources* are 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



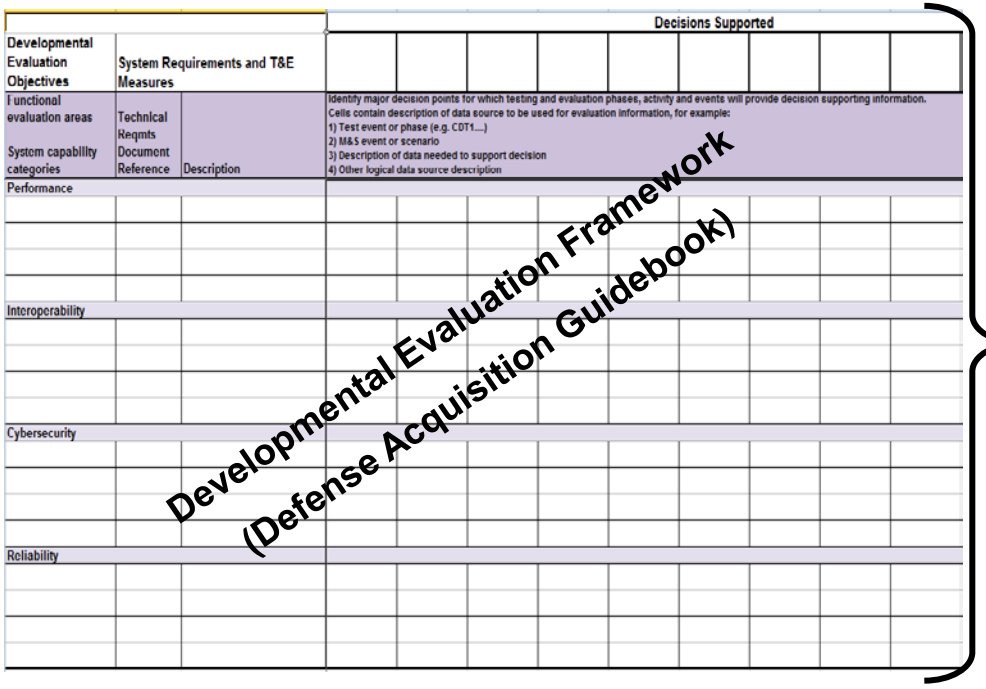
DT&E story thread: decision – evaluation– test & resources

Developmental Evaluation Framework

(Enclosure 4, DoD Interim Instruction 5000.02)

Test and Evaluation Master Plan (TEMP) includes a Developmental Evaluation Framework ("T&E Roadmap")

- **Knowledge gained from testing provides information for technical, programmatic, and acquisition decisions.**

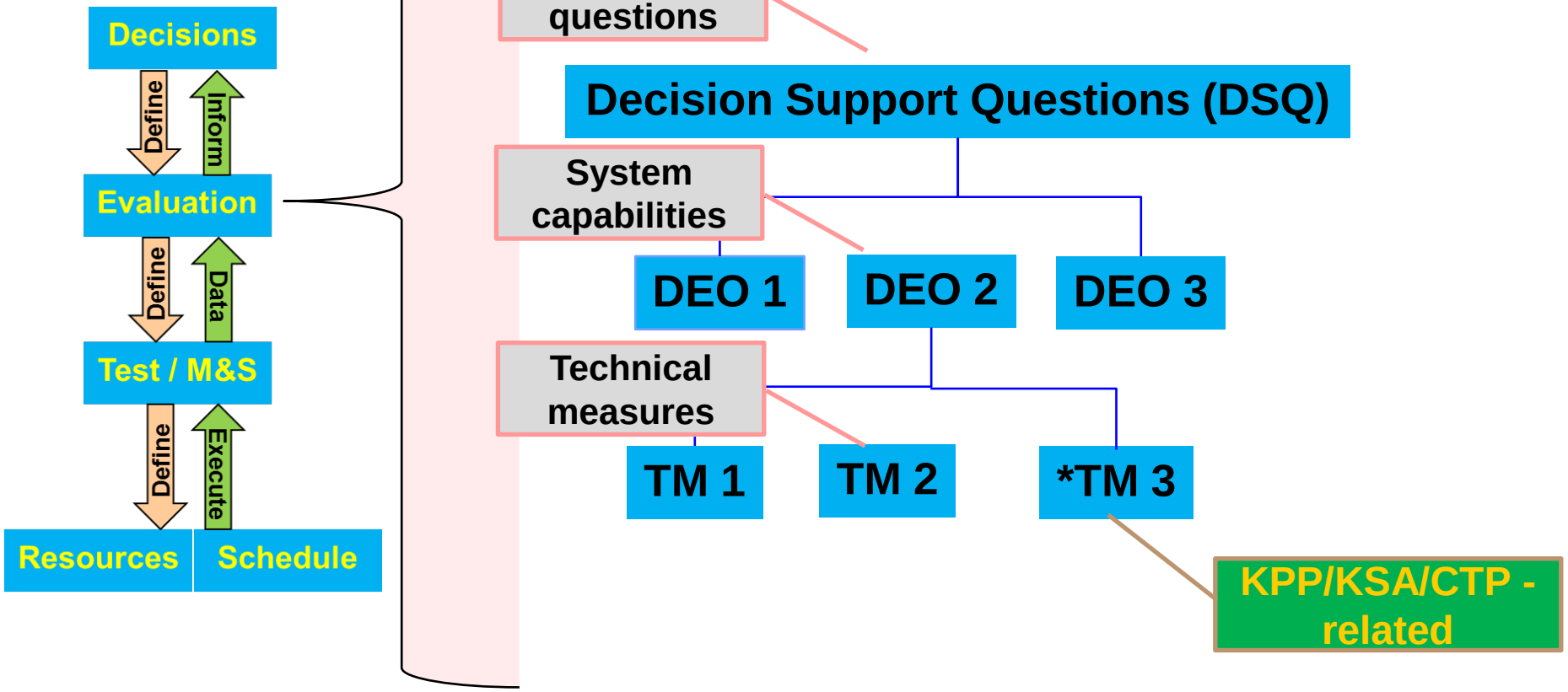


DoDI 5000.02 (Interim)

Developmental Evaluation Framework:

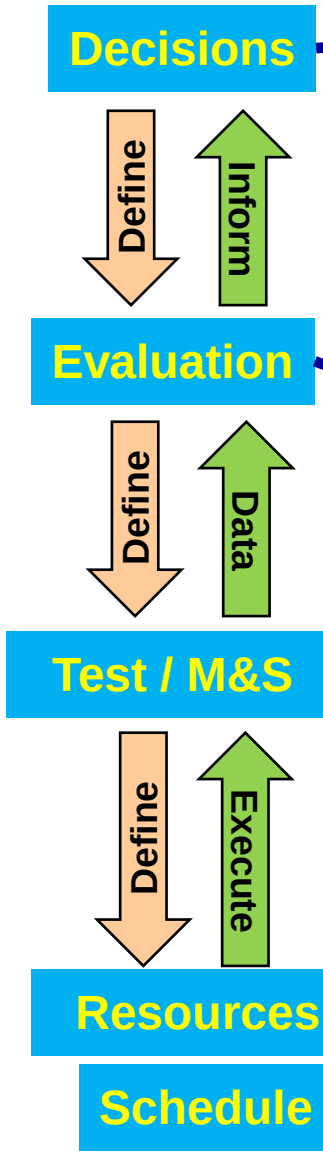
- Identifies key data that contributes to assessing progress on:
  - Key Performance Parameters
  - Critical Technical Parameters
  - Key System Attributes
  - Interoperability requirements
  - Cybersecurity requirements
  - Reliability growth
  - Maintainability attributes
  - Developmental test objectives
  - Others as needed
- Show the correlation/mapping between:
  - Test events
  - Key resources
  - Decision supported

Developmental Evaluation Framework (DEF)



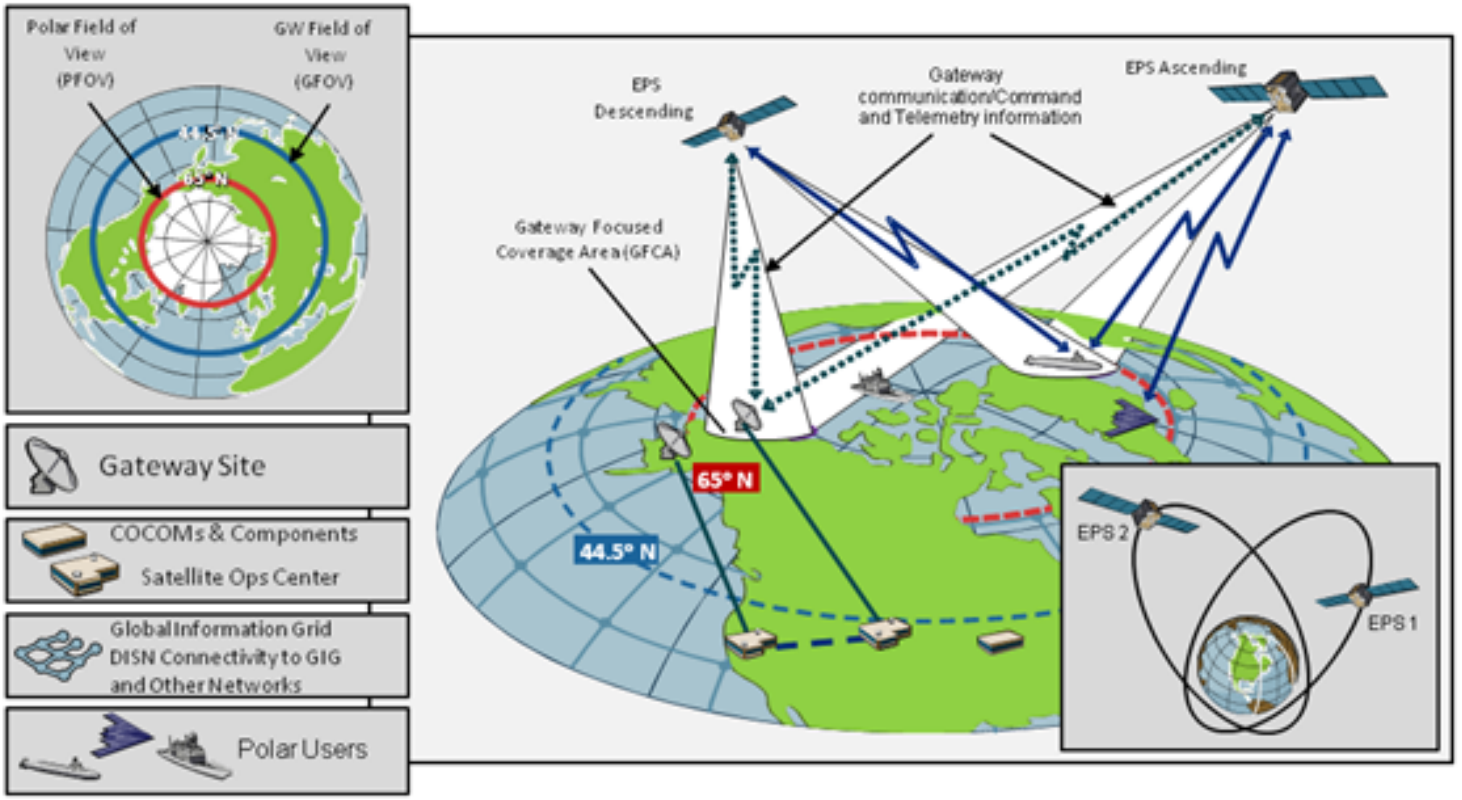
System Engineering decomposition:
Evaluate system capability - Inform decisions

Developmental Evaluation Framework



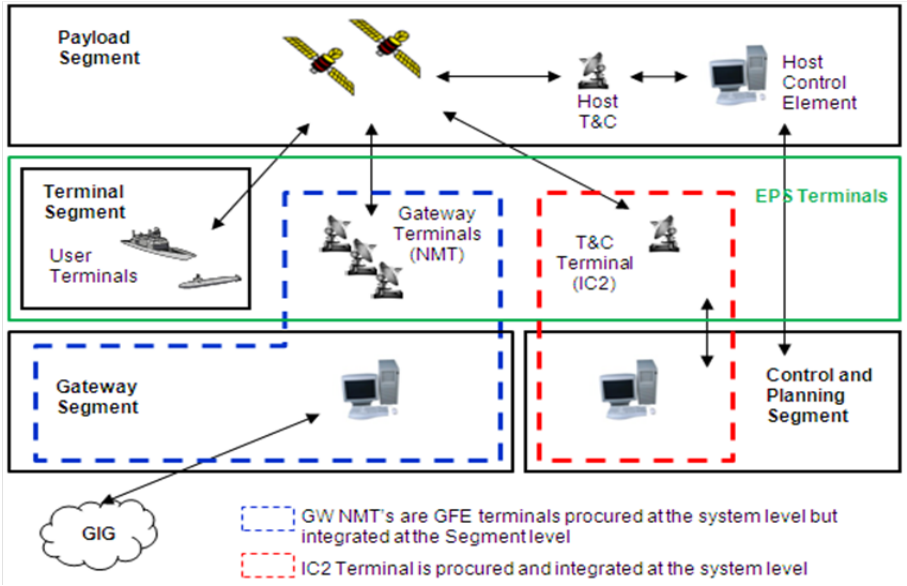
Developmental Evaluation Objectives	System Requirements and T&E Measures		Decisions Supported							
			Decision #1		Decision #2			Decision #3	Decision #4	
			DSQ #1	DSQ #2	DSQ #3	DSQ #4	DSQ #5	DSQ #6	DSQ #7	DSQ #8
Functional evaluation areas System capability categories	Technical Reqmts Document Reference	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 – Enhanced Polar System



Protected SATCOM (EHF) for polar-region users consisting of 4 segments: EPS Payload Segment, EPS Terminal Segment, EPS Control and Planning Segment (CAPS), EPS Gateway Segment

Inform Capability & Integration Decisions



Can the terminals ***communicate*** with the payloads?

Is CAPS capable of ***mission planning***?

Can CAPS ***command and control*** PL using ***in-band?***

Is CAPS capable of utilizing ***out-of-band T&C*** through the Host Interface?

Is the ***Gateway*** capable of ***connecting*** polar users and mid-lat users?

Is EPS ***secure***?

Is EPS ***sustainable***?

EPS Developmental Evaluation Framework

Enterprise DSQs

Linked Integrated System Tests

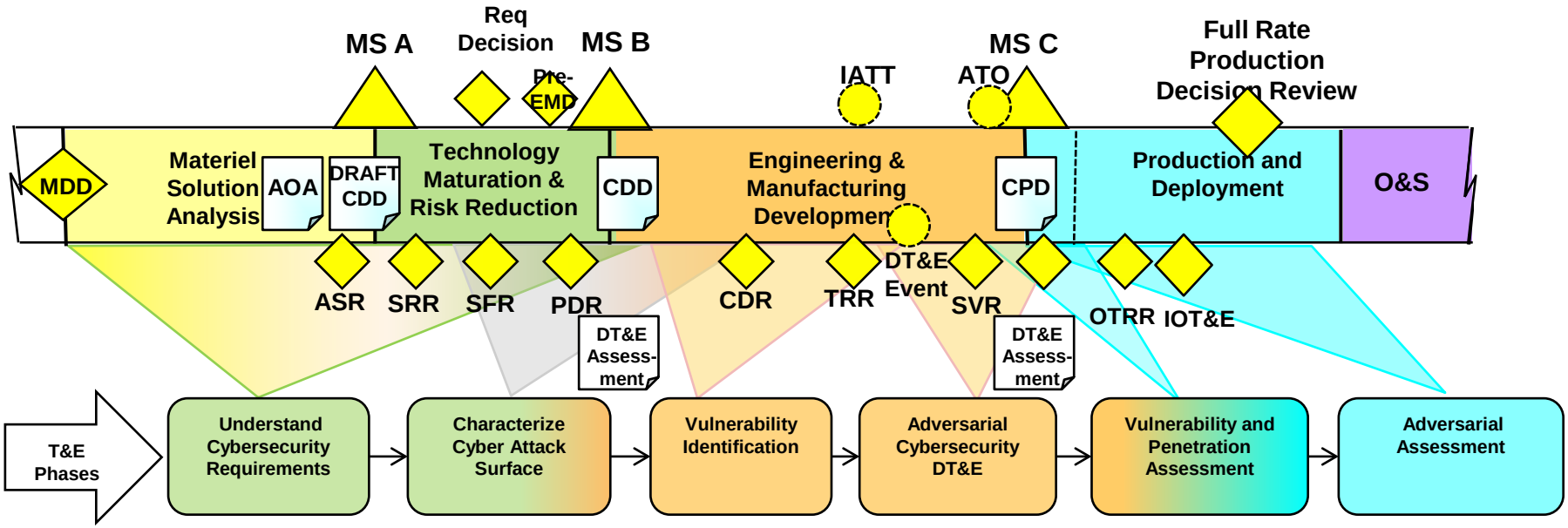
System capabilities (DEOs)

TM to evaluate DEO/DSQ

KPP/KSA associated TM highlighted

	Critical Developmental Issues (Enterprise)	*Can terminals communicate with PL?*	*Is CAPS capable of mission planning?*	*Can CAPS command and control PL using in-band?*	*Is CAPS capable of utilizing out-of-band T&C through the Host interface?*	*Is GW capable of connecting polar users and mid-lat users?*	*Is EPS secure?*	*Is B su abl*
	Integration Test Event	ISTs E0100/ E0830	IST E0250	ISTs E0250/E0810	ISTs E0350/E0800	GW FQT/IQT/IST E0830	GW FQT/CAPS FAT/IST E0280	PAR/GW FQT/CAPS FAT
Objectives	**Measures***							
Capacity and throughput	**Full Service Capacity**	x	x	x		x		
	GW Throughput					x		
	CAPS Max CPU Utilization			x				
	# of planned and active Terminals	x	x	x				
Coverage	Constellation	x	x	x	x	x		
	Service Coverage Region	x	x	x		x		
Unstressed Communications	Data rate, Error Rate, EIRP, RRIP, **Uplink**	x	x	x			x	

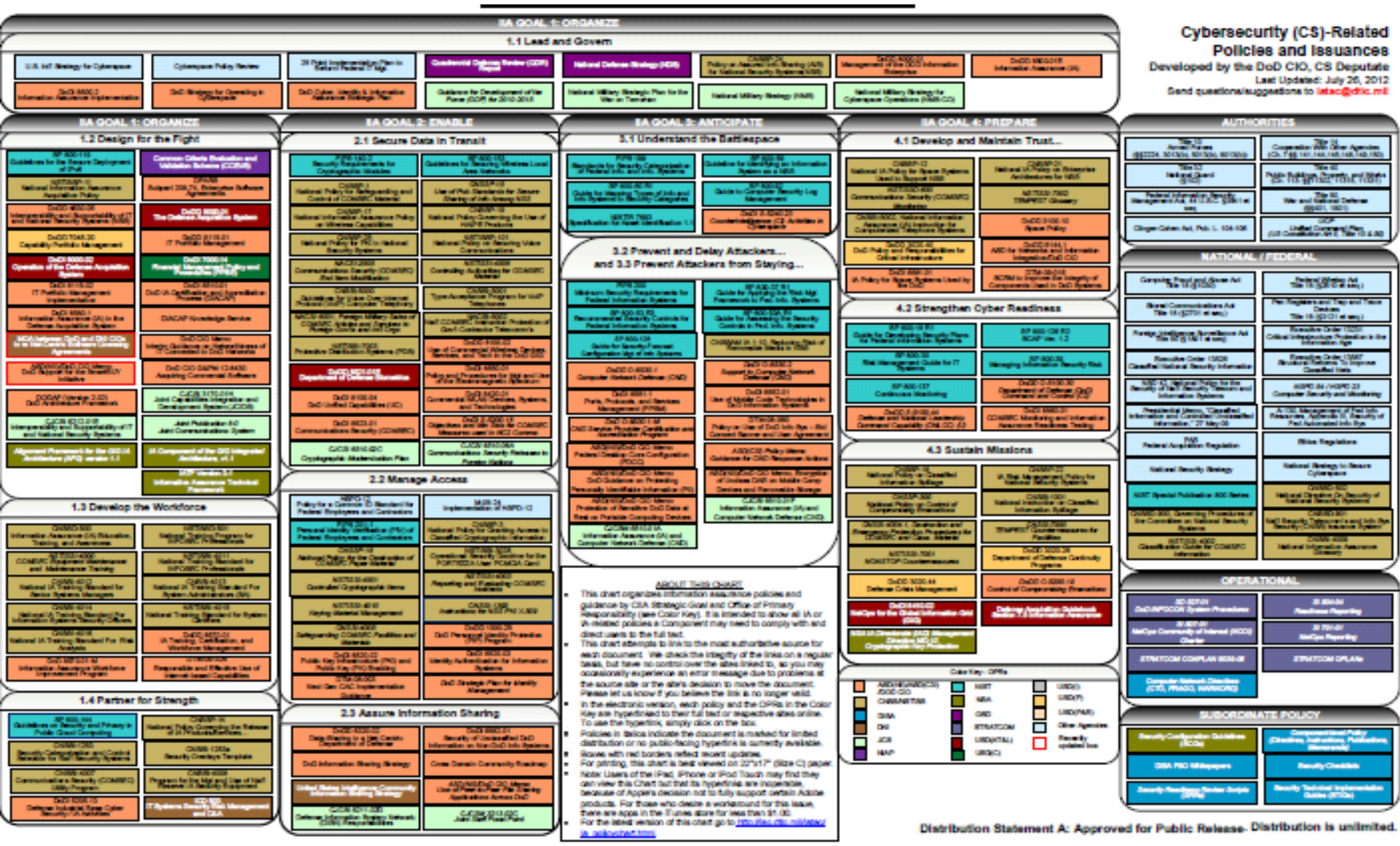
Cybersecurity T&E Phases Start Before & Build on PPP and RMF!



- **Phases as depicted are mapped to milestones and design reviews**
  - **Programs have latitude on timing of Phases**
- **Phases are iterative and should be iterated as system matures**
  - **SE and T&E Stakeholders collaborate to iterate process**
- **Build in "fix-it" intervals**
  - ***Shift "vulnerability discovery" earlier in acquisition life cycle***

Approved for Public Release; Distribution Unlimited. 14-1912

IA Policy Guidance "Shock & Awe"



Cyber EF Roadmap Guides T&E Path

Cyber Evaluation Framework Expands on DEF's "Security" DSQ

		Critical Developmental Issues (Enterprise)	*Can terminals communicate with PL?*	*Is CAPS capable of mission planning?*	*Can CAPS command and control PL using in-band?*	*Is CAPS capable of utilizing out-of-band T&C through the Host interface?*	*Is GW capable of connecting polar users and mid-lat users?*	*Is EPS secure?*	*Is EPS sustainable?*
	Integration Test Event	ISTs E0100/ E0830	IST E0250	ISTs E0250/E0810	ISTs E0350/E0800	GW FQT/IQT/IST E0830	GW FQT/CAPS FAT/IST E0280		
Developmental Test Objectives	**Measures***								
Capacity and throughput	**Full Service Capacity**	x	x	x		x			
	GW Throughput					x			
	CAPS Max CPU Utilization			x					
	# of planned and active Terminals	x	x	x					
Coverage	Constellation	x	x	x					
	Service Coverage Region	x	x	x					
Unstressed Communications	Data rate, Error Rate, EIRP, RRIP, **Uplink**	x	x	x					

Cyber Technical Capability/ Evaluation Activity Categories	DT Objectives - Cyber Technical Capabilities	Is the system and software developed securely?	Does [illegible] baseli[illegible] techni[illegible]	[illegible]IA	Do exposed vulnerabilities adversely effect system resiliency?	Is the system mission capable and interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?	Test Activity / Data Source
Systems and Software Assurance	Software Vulnerabilities Mitigated in critical components	Program Protection Plan (PPP) Table 5.3.3. Example Software Metrics include: Number/Category outstanding SDRs % Code Static Analysis Planned/Inspected % Code Planned/Inspected %SW LOC Planned/Inspected CVE %SW LOC Planned/Inspected CAPEC %SW LOC Planned/Inspected CWE %SW LOC Planned/Pen Tested %SW LOC Tested (Coverage)					Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Software Vulnerabilities Mitigated in Operational System	PPP Table 5.3.3 Example Operational System Metrics for CPI, Critical Functions, Developmental SW and COTS/NDI include: Fault Isolation Planned/Implemented Least Privilege Planned/Implemented System Element Isolation Planned/Implemented Input Checking/Validation Planned/Implemented SW Load Key (Signed) Planned/Implemented					Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Software Vulnerabilities Mitigated in Development Environment	PPP Table 5.3.3 Example Development Environment Metrics based upon SW Products selected including Compiler, Automated Testing Tools, Configuration Management System, Test Results Database, etc.					Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Anti-Tamper Vulnerbailties Mitigated	PPP Table 5.3.3, PPP Section 5.3.1 and/or Appendix D: Anti-tamper Plan. Metrics derived for appropriate CPI, Critical Components					Anti-Tamper Implementation Plan/Report PPP, CDRLs from CTR and government.
	Supply Chain Risks Mitigated	PPP Section 5.3.4 Supply Chain Risk Management (SCRM) Metrics derived from SCRM V&V Plan for appropriate CPI, Critical Components etc.					Supply Chain Risk Management/Reports PPP, CDRLs from CTR and government.
RMF Controls and Attack Surface Standards Verification	RMF Control Categories include: Access Control Awareness and Training Audit and Accountability Configuration Management Contingency Planning Identification and Authentication Incident Response Media Protection Maintenance Physical and Environmental Protection Planning Security Assessment and Authorization Personnel Security Risk Assessment System and Services Acquisition System and Communications Protection System and Information Integrity Program Management		RMF Metrics and measures can be derived from several source documents including Capabilities Documents, PPP, Cybersecurity Strategy, Security Controls Assessment Plan, Performance Specifications etc. Example metrics by control category may include: % of controls verified # and Category Deficiencies % of inherited controls verified # and Category Inherited Deficiencies			ST&E/ Security Controls Assessor/ Step 3/4 Vulnerability Assessment
	Attack surfaces to be evaluated based on Step 2 analysis. Potential Attack Surfaces include: Connecting systems explicitly identified in Cybersecurity Strategy RF Interfaces (Data Links, Wi-Fi, Bluetooth) SCADA Interfaces (Control Net, Device Net, Fieldbus, Zig Bee, etc.)		Metrics and measures can be developed from DIACAP/RMF and technical standards appropriate for the exposed Attack Surface.			ST&E/ Security Controls Assessor/Step 3 Vulnerability Assessment. Contractor ST&E and Government Technical Standards Testing as appropriate
Cyber Kill Chain Vulnerability Assessment	Cyber Kill Chain Vulnerability and System Interoperability and functionality in response to exploited cyber vulnerabilities shall be evaluated in operational scenarios: 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 in collaboration with other program stakeholders. Critical Missions may be derived from CONOPS, Capabilities Documents, PPP, etc. 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 net-centric 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 Cyber Threat Defense Science Board Task Force. The below measures are derived from MP 120053, Rev 1, Cyber Resiliency Metrics, dated Apr 2012. Additional metrics will be selected by the ITT in collaboration with other Stakeholders. Initial planned metrics include: - % cyber resources properly configured (Configuration varies by resource) - % attempted intrusions stopped at network perimeter/ deflected - % mission-essential capabilities for which multiple instantiations available - Avg Length of time between initial disruption and restoration - Quality of restored data - Quality of choices made during design and engineering that affect resiliency - % mission-essential datasets for which all items effectively have two or more independent external data feeds - % mission-essential data stores for which a master copy exists - % data value assertions in a mission-essential data store for which a master copy exists	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 functions as an adversary without knowledge or access to the system (Red Team)

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 5.3.3.-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 5.3.4				Supply Chain Risk Management/Report
(DIACAP) DOD 8500/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: % of controls verified, number/category of outstanding deficiencies)			ST&E/ Security Controls Assessor/ 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 net-centric 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 Cyber Threat Defense Science Board Task Force. The below measures are derived from NP 120053. Rev 1. Cyber Resiliency Metrics. dated Apr 2012. Example metrics include: - % cyber resources properly configured - # attempted intrusions stopped at network perimeter/ deflected to honeypot - % 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 - % mission-essential datasets for which all items effectively have two or more independent external data feeds - % mission-essential data stores for which a master copy exists - % 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 functions as an adversary without knowledge or access to the System (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

Critical Developmental Issue Technical Capability	DT Objectives - Cyber Technical Capabilities	Example Metrics and Measures	Test Phase / Data Source
Is the system and software developed securely? Systems and Software Assurance	Software Vulnerabilities Mitigated in critical components	Program Protection Plan (PPP) Table 5.3.3. Example Software Metrics include: Quality Metrics, Number/Category outstanding SDRs etc. Security Metrics including: % Code Static Analysis Planned/Inspected % Code Planned/Inspected %SW LOC Planned/Inspected CVE %SW LOC Planned/Inspected CAPEC %SW LOC Planned/Inspected CWE %SW LOC Planned/Pen Tested %SW LOC Tested (Coverage)	Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Software Vulnerabilities Mitigated in Operational System	PPP Table 5.3.3 Example Operational System Metrics for CPI, Critical Functions, Developmental SW and COTS/NDI include: Fault Isolation Planned/Implemented Least Privilege Planned/Implemented System Element Isolation Planned/Implemented Input Checking/Validation Planned/Implemented SW Load Key (Signed) Planned/Implemented	
	Software Vulnerabilities Mitigated in Dev. Environment	PPP Table 5.3.3 Example Development Environment Metrics based upon SW Products selected including Compiler, Automated Testing Tools, Configuration Management System, Test Results Database, etc.	
	Anti-Tamper Vulnerabilities Mitigated	PPP Table 5.3.3, PPP Section 5.3.1 and/or Appendix D: Anti-tamper Plan. Metrics derived for appropriate CPI, Critical Components	Anti-Tamper Implementation Plan/Report, PPP, CDRLs from CTR and government.
	Supply Chain Risks Mitigated	PPP Section 5.3.4 Supply Chain Risk Management (SCRM) Metrics derived from SCRM V&V Plan for appropriate CPI, Critical Components etc.	Supply Chain Risk Management Plan/Reports, PPP, CDRLs from CTR and government.

Risk Management Framework

Critical Developmental Issue Technical Capability	DT Objectives - Cyber Technical Capabilities	Example Metrics and Measures	Test Phase / Data Source
Does the system and associated Attack Surfaces/Interfaces satisfy baseline Cybersecurity technical standards? RMF Controls and Attack Surface Standards Verification and Validation	RMF Control Categories include: Access Control Awareness and Training Audit and Accountability Configuration Management Contingency Planning Identification and Authentication Incident Response Media Protection Maintenance Physical and Environmental Protection Planning Security Assessment and Authorization Personnel Security Risk Assessment System and Services Acquisition System and Communications Protection System and Information Integrity Program Management	RMF Metrics and measures can be derived from several source documents including Capabilities Documents, PPP, Cybersecurity Strategy, Security Controls Assessment Plan/Reports, Performance Specifications etc. Example metrics by control category may include: % of controls verified # and Category Deficiencies % of inherited controls verified # and Category Inherited Deficiencies Authority to Operate/test	ST&E/ Security Controls Assessor/ Phase 3/4 Vulnerability Assessment
	Attack surfaces to be evaluated based on Phase 2 analysis. Potential Attack Surfaces include: Connecting systems explicitly identified in Cybersecurity Strategy RF Interfaces (Data Links, Wi-Fi, Bluetooth) SCADA Interfaces (Control Net, Device Net, Fieldbus, Zig Bee, etc.)	RMF Metrics and measures for connecting systems may include: % of controls verified # and Category Deficiencies % of inherited controls verified # and Category Inherited Deficiencies Authority to Operate/Test *Attack Surface Measures and Metrics should be developed based upon the Security Technical Standards for the interface*	ST&E/ Security Controls Assessor/Phase 3 Vulnerability Assessment, Contractor ST&E and Government Technical Standards Testing as appropriate

Vulnerability Assessment

Critical Developmental Issue Technical Capability	DT Objectives - Cyber Technical Capabilities	Example Metrics and Measures	Test Phase / Data Source
Do exposed vulnerabilities adversely effect system resiliency? Cyber Kill Chain Vulnerability Assessment Cyber kill chain as exercised by the adversary includes the following Activities: 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. Cyber Defense actions describe the intended effects of Cyber Resiliency Techniques on Adversary Activities	Cyber Kill Chain assessment in response to exploited cyber vulnerabilities shall be evaluated in operational scenarios. 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, Cybersecurity CONOPS and cyber attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source.	ITT will develop measures in collaboration with other program stakeholders. Critical Missions may be derived from CONOPS, Capabilities Documents, PPP, etc. 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 net-centric military operations. Cyber Kill Chain Metrics and measures may be derived from Cybersecurity CONOPS, Program technical documentation etc. Example metrics follow: # and % Resources properly configured (Configuration, STIG for example, varies by resource) # and % reconnaissance attempts stopped at network perimeter/deflected # and % deliveries stopped at network perimeter/deflected # and % exploits stopped before execution # and % attempted intrusions stopped at network perimeter/deflected # and % intrusions detected Avg Length of time between intrusion/disruption and detection Avg Length of time intrusion/disruption and restoration # and % data exfiltrations detected # and % data exfiltrations stopped % mission-essential capabilities for which multiple instantiations available Integrity/Quality of restored data % mission-essential datasets with multiple/independent external data feeds % mission-essential data stores with master copy (Backups)	Phase 3 Vulnerability Assessment Team has full knowledge and access to the System and all supporting components (Blue Team)

Interoperability & Exploited Cyber Vulnerabilities

Critical Developmental Issue Technical Capability	DT Objectives - Cyber Technical Capabilities	Example Metrics and Measures	Test Phase / Data Source
Is the system mission capable and interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities? System interoperability and functionality in response to exploited cyber vulnerabilities Cyber kill chain as exercised by the adversary includes the following Activities: 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. Cyber Defense actions describe the intended effects of Cyber Resiliency Techniques on Adversary Activities	System Interoperability and functionality in response to exploited cyber vulnerabilities shall be evaluated in operational scenarios. 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, Cybersecurity CONOPS and cyber attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source.	ITT will develop measures in collaboration with other program stakeholders. Critical Missions may be derived from CONOPS, Capabilities Documents, PPP, etc. 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 net-centric military operations. Cyber Kill Chain Metrics and measures may be derived from Cybersecurity CONOPS, Program technical documentation etc. Example metrics follow: # and % Resources properly configured (Configuration, STIG for example, varies by resource) # and % reconnaissance attempts stopped at network perimeter/deflected # and % attack deliveries stopped at network perimeter/deflected # and % exploits stopped before execution # and % attempted intrusions stopped at network perimeter/deflected # and % intrusions detected Avg Length of time between intrusion/disruption and detection Avg Length of time intrusion/disruption and restoration # and % data exfiltrations detected # and % data exfiltrations stopped % mission-essential capabilities for which multiple instantiations available Integrity/Quality of restored data % mission-essential datasets with multiple/independent external data feeds % mission-essential data stores with master copy (Backups)	Phase 4 Vulnerability Assessment: Team functions as an adversary (Red Team)

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