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
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
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

Capabilities questions

Decision Support Questions (DSQ)

System capabilities

Technical measures

DEO 1
DEO 2
DEO 3

TM 1
TM 2
*TM 3

KPP/KSA/CTP - related
### Developmental Evaluation Framework

<table>
<thead>
<tr>
<th>Developmental Evaluation Objectives</th>
<th>System Requirements and T&amp;E Measures</th>
<th>Decisions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functional evaluation areas</strong></td>
<td><strong>Technical Reqmts</strong> Document Reference Description</td>
<td>Decision #1</td>
</tr>
<tr>
<td><strong>System capability categories</strong></td>
<td><strong>Description</strong></td>
<td>DSQ #1</td>
</tr>
<tr>
<td>Performance</td>
<td>DT#1 Technical Measure #1</td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td>DT#1 M&amp;S#4 Technical Measure #2</td>
<td></td>
</tr>
<tr>
<td>Interoperability</td>
<td>DT#3 Technical Measure #3</td>
<td></td>
</tr>
<tr>
<td>Interoperability</td>
<td>DT#4 Technical Measure #4</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>SW Assurance Measure #1</td>
<td></td>
</tr>
<tr>
<td>Reliability Cap #1</td>
<td>Technical Measure #11</td>
<td></td>
</tr>
<tr>
<td>Reliability Cap #2</td>
<td>Technical Measure #12</td>
<td></td>
</tr>
<tr>
<td>Reliability Cap #3</td>
<td>Technical Measure #13</td>
<td></td>
</tr>
<tr>
<td>Reliability Cap #4</td>
<td>Technical Measure #14</td>
<td></td>
</tr>
</tbody>
</table>

**Cell Reference:**
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 

---

**Define**
- Inform
- Data

**Test / M&S**
- Define
- Execute

**Evaluation**
- Define
- Data

**Resources**
- Define
- Schedule
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
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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Test Event</td>
<td>ISTs E0100/ E0830</td>
<td>IST E0250</td>
<td>ISTs E0250/E0810</td>
<td>ISTs E0350/E0800</td>
<td>GW FQT/IQT/IST E0830</td>
<td>GW FQT/CAST FAT/IST E0280</td>
</tr>
</tbody>
</table>

### System capabilities (DEOs)

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Measures*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity and throughput</td>
<td>Full Service Capacity</td>
</tr>
<tr>
<td></td>
<td>GW Throughput</td>
</tr>
<tr>
<td></td>
<td>CAPS Max CPU Utilization</td>
</tr>
<tr>
<td></td>
<td># of planned and active Terminals</td>
</tr>
<tr>
<td>Coverage</td>
<td>Constellation</td>
</tr>
<tr>
<td></td>
<td>Service Coverage Region</td>
</tr>
<tr>
<td>Unstressed Communications</td>
<td>Data rate, Error Rate, EIRP, RRIP, Uplink</td>
</tr>
</tbody>
</table>

*Linked Integrated System Tests

*TM to evaluate DEO/DSQ

*Enterprise DSQs

*KPP/KSA associated TM highlighted
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*
IA Policy Guidance “Shock & Awe”
Cyber EF Roadmap Guides
T&E Path
Expands on DEF’s “Security” DSQ Cyber Evaluation Framework

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Test Event</td>
<td>ISTs E0100/E0830</td>
<td>IST E0250</td>
<td>ISTs E0250/E0830</td>
<td>ISTs E0250/E0830</td>
<td>GW FQT/QT/IST E0830</td>
<td>GW FQT/QT/IST E0830</td>
<td>GW CAPS FAT/IST E0830</td>
</tr>
</tbody>
</table>

### Developmental Test Objectives

<table>
<thead>
<tr>
<th>Measures</th>
<th>Full Service Capacity</th>
<th>GW Throughput</th>
<th>CAPS Max CPU Utilization</th>
<th># of planned and active Terminals</th>
<th>Constellation</th>
<th>Service Coverage Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Cyber Evaluation Framework

Expands on DEF’s “Security” DSQ Cyber Evaluation Framework.

1. **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 connecting out-of-band T&Cs through the host interface?
   - Is GW capable of connecting polar users and mid-lat users?
   - Is EPS secure?
   - Is EPS sustainable?

2. **Integration Test Event**
   - ISTs E0100/E0830
   - IST E0250
   - ISTs E0250/E0830
   - ISTs E0250/E0830
   - GW FQT/QT/IST E0830
   - GW FQT/QT/IST E0830
   - GW CAPS FAT/IST E0830
   - GW CAPS FAT/IST E0830

3. **Developmental Test Objectives**
   - Measures
     - Full Service Capacity
     - GW Throughput
     - CAPS Max CPU Utilization
     - # of planned and active Terminals
     - Constellation
     - Service Coverage Region
     - Unstressed Communications
       - Data rate
       - Error Rate
       - EIRP
       - RRI
       - Uplink

4. **Developmental Capability/Technical Authority Categories**
   - Defends the system and software development process.

5. **Contractor T&E/ Governmental/Contractor FQT/ Governmental**
   - Critical Missions
   - Support Net-Centric Military Operations
   - Support Centric Military Operations
   - Support Traditional Military Operations

### Cyber Security Metrics and Measures

- **Critical Missions**
  - % of controls verified
  - # of controls verified
  - # of Category Inherited Deficiencies
  - # of Category Outstanding SDRs

- **Support Net-Centric Military Operations**
  - % of mission-essential datasets for which all data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential capabilities for which data value assertions in a master copy exists

- **Support Traditional Military Operations**
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists

### Example Operational System Metrics

- SW Load Key (Signed) Planned/Implemented
- Input Checking/Validation Planned/Implemented
- Fault Isolation Planned/Implemented
- COTS/NDI

### Example Metrics by Control

- Performance Specifications
- Controls Assessment Plan
- Cybersecurity Strategy, Security Capabilities Documents, PPP, etc.

### Additional Metrics

- Interoperability metrics
- Critical Missions in Interoperability
- Interoperability in response to vulnerabilities
- Interoperability in response to modifications

### Contractor T&E/ Governmental/Qualification Testing

- Functional
- Technical
- Security
- Performance
- Special Operations

### System and Information Integrity

- System and Services Acquisition
- Risk Assessment
- Program Management
- Supply Chain Risk Management
- Reports

### System and Services Acquisition

- Critical Missions
- Support Net-Centric Military Operations
- Support Traditional Military Operations
- Support Centric Military Operations

### Risk Assessment

- Threat Defense Science Board Task Force
- Additional metrics will be selected by the ITT in planned metrics include:
  - %SW LOC Tested (Coverage)
  - %SW LOC Planned/Inspected
  - %SW LOC Planned/Inspected
  - % Code Planned/Inspected
  - % SW Load Key (Signed) Planned/Implemented
  - Input Checking/Validation Planned/Implemented
  - Fault Isolation Planned/Implemented

### Example Metrics

- Critical Missions
  - % of controls verified
  - # of controls verified
  - # of Category Inherited Deficiencies
  - # of Category Outstanding SDRs

- Support Net-Centric Military Operations
  - % of mission-essential datasets for which all data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential capabilities for which data value assertions in a master copy exists

- Support Traditional Military Operations
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists

### Critical Missions

- % of mission-essential datasets for which all data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists
- % of mission-essential capabilities for which data value assertions in a master copy exists

### Support Net-Centric Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Support Traditional Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Example Metrics

- Performance Specifications
- Controls Assessment Plan
- Cybersecurity Strategy, Security Capabilities Documents, PPP, etc.

### Additional Metrics

- Interoperability metrics
- Critical Missions in Interoperability
- Interoperability in response to vulnerabilities
- Interoperability in response to modifications

### Contractor T&E/ Governmental/Qualification Testing

- Functional
- Technical
- Security
- Performance
- Special Operations

### System and Information Integrity

- System and Services Acquisition
- Risk Assessment
- Program Management
- Supply Chain Risk Management
- Reports

### System and Services Acquisition

- Critical Missions
- Support Net-Centric Military Operations
- Support Traditional Military Operations
- Support Centric Military Operations

### Risk Assessment

- Threat Defense Science Board Task Force
- Additional metrics will be selected by the ITT in planned metrics include:
  - %SW LOC Tested (Coverage)
  - %SW LOC Planned/Inspected
  - %SW LOC Planned/Inspected
  - % Code Planned/Inspected
  - % SW Load Key (Signed) Planned/Implemented
  - Input Checking/Validation Planned/Implemented
  - Fault Isolation Planned/Implemented
  - COTS/NDI

### Example Metrics

- Critical Missions
  - % of controls verified
  - # of controls verified
  - # of Category Inherited Deficiencies
  - # of Category Outstanding SDRs

- Support Net-Centric Military Operations
  - % of mission-essential datasets for which all data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential capabilities for which data value assertions in a master copy exists

- Support Traditional Military Operations
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists

### Example Metrics

- Performance Specifications
- Controls Assessment Plan
- Cybersecurity Strategy, Security Capabilities Documents, PPP, etc.

### Additional Metrics

- Interoperability metrics
- Critical Missions in Interoperability
- Interoperability in response to vulnerabilities
- Interoperability in response to modifications

### Contractor T&E/ Governmental/Qualification Testing

- Functional
- Technical
- Security
- Performance
- Special Operations

### System and Information Integrity

- System and Services Acquisition
- Risk Assessment
- Program Management
- Supply Chain Risk Management
- Reports

### Example Metrics

- Critical Missions
  - % of controls verified
  - # of controls verified
  - # of Category Inherited Deficiencies
  - # of Category Outstanding SDRs

- Support Net-Centric Military Operations
  - % of mission-essential datasets for which all data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential capabilities for which data value assertions in a master copy exists

- Support Traditional Military Operations
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists

### Critical Missions

- % of mission-essential datasets for which all data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists
- % of mission-essential capabilities for which data value assertions in a master copy exists

### Support Net-Centric Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Support Traditional Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Example Metrics

- Performance Specifications
- Controls Assessment Plan
- Cybersecurity Strategy, Security Capabilities Documents, PPP, etc.

### Additional Metrics

- Interoperability metrics
- Critical Missions in Interoperability
- Interoperability in response to vulnerabilities
- Interoperability in response to modifications

### Contractor T&E/ Governmental/Qualification Testing

- Functional
- Technical
- Security
- Performance
- Special Operations

### System and Information Integrity

- System and Services Acquisition
- Risk Assessment
- Program Management
- Supply Chain Risk Management
- Reports

### Example Metrics

- Critical Missions
  - % of controls verified
  - # of controls verified
  - # of Category Inherited Deficiencies
  - # of Category Outstanding SDRs

- Support Net-Centric Military Operations
  - % of mission-essential datasets for which all data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential capabilities for which data value assertions in a master copy exists

- Support Traditional Military Operations
  - % of mission-essential data stores for which a master copy exists
  - % of mission-essential data stores for which a master copy exists

### Critical Missions

- % of mission-essential datasets for which all data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists
- % of mission-essential capabilities for which data value assertions in a master copy exists

### Support Net-Centric Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Support Traditional Military Operations

- % of mission-essential data stores for which a master copy exists
- % of mission-essential data stores for which a master copy exists

### Example Metrics

- Performance Specifications
- Controls Assessment Plan
- Cybersecurity Strategy, Security Capabilities Documents, PPP, etc.
## Cyber EF Roadmap Use

**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

---

### Cyber Technical Capability Evaluation Activity Categories

<table>
<thead>
<tr>
<th>Categories</th>
<th>System Assurance</th>
<th>Compliance (C&amp;A, RMF)</th>
<th>Vulnerability Assessment (Red team, Blue team)</th>
<th>Interoperability (NR-KPP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Objectives/Cyber Technical Capabilities</td>
<td>Program Protection Plans (PPPs) Table 5.3.3: (example measures: number/cally of SIOs, OISs abolished, OISs remaining, CPEGS modified)</td>
<td>Appendix C: Anti-tamper plan</td>
<td>Anti-Tamper Implementation Plan/Report</td>
<td></td>
</tr>
</tbody>
</table>

**Source documents, examples of measures**
- Test activities, data sources

---

**Test Activity/Data Source**
- Contractor FCI Functional Qualification Testing (FCQF) Government STKeM
- SRAE/Security Controls Assessment/Audit Step 3 vulnerability assessment 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
<table>
<thead>
<tr>
<th>Critical Developmental Issue Technical Capability</th>
<th>DT Objectives - Cyber Technical Capabilities</th>
<th>Example Metrics and Measures</th>
<th>Test Phase / Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the system and software developed securely?</td>
<td>Software Vulnerabilities Mitigated in critical components</td>
<td>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)</td>
<td>Contractor T&amp;E/ Functional Qualification Testing (FQT)/ Government ST&amp;E PPP, CDRLs from CTR and government.</td>
</tr>
<tr>
<td>Systems and Software Assurance</td>
<td>Software Vulnerabilities Mitigated in Operational System</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software Vulnerabilities Mitigated in Dev. Environment</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Tamper Vulnerabilities Mitigated</td>
<td>PPP Table 5.3.3, PPP Section 5.3.1 and/or Appendix D: Anti-tamper Plan. Metrics derived for appropriate CPI, Critical Components</td>
<td>Anti-Tamper Implementation Plan/Report, PPP, CDRLs from CTR and government.</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risks Mitigated</td>
<td>PPP Section 5.3.4 Supply Chain Risk Management (SCRM) Metrics derived from SCRM V&amp;V Plan for appropriate CPI, Critical Components etc.</td>
<td>Supply Chain Risk Management Plan/Reports, PPP, CDRLs from CTR and government.</td>
</tr>
</tbody>
</table>
### Risk Management Framework

<table>
<thead>
<tr>
<th>Critical Developmental Issue Technical Capability</th>
<th>DT Objectives - Cyber Technical Capabilities</th>
<th>Example Metrics and Measures</th>
<th>Test Phase / Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system and associated Attack Surfaces/Interfaces satisfy baseline Cybersecurity technical standards?</td>
<td>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. <strong>Attack surfaces to be evaluated based on Phase 2 analysis. Potential Attack Surfaces include:</strong> Connecting systems explicitly identified in Cybersecurity Strategy, RF Interfaces (Data Links, Wi-Fi, Bluetooth), SCADA Interfaces (Control Net, Device Net, Fieldbus, Zig Bee, etc.)</td>
<td>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</td>
<td>ST&amp;E/ Security Controls Assessor/Phase 3/4 Vulnerability Assessment</td>
</tr>
<tr>
<td>RMF Controls and Attack Surface Standards Verification and Validation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.**
## Vulnerability Assessment

<table>
<thead>
<tr>
<th>Critical Developmental Issue Technical Capability</th>
<th>DT Objectives - Cyber Technical Capabilities</th>
<th>Example Metrics and Measures</th>
<th>Test Phase / Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do exposed vulnerabilities adversely effect system resiliency?</td>
<td>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.</td>
<td>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)</td>
<td>Phase 3 Vulnerability Assessment Team has full knowledge and access to the System and all supporting components (Blue Team)</td>
</tr>
</tbody>
</table>

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.
# Interoperability & Exploited Cyber Vulnerabilities

<table>
<thead>
<tr>
<th>Critical Developmental Issue Technical Capability</th>
<th>DT Objectives - Cyber Technical Capabilities</th>
<th>Example Metrics and Measures</th>
<th>Test Phase / Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the system mission capable and interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?</td>
<td>System Interoperability and functionality in response to exploited cyber vulnerabilities shall be evaluated in operational scenarios.</td>
<td>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.</td>
<td>Phase 4 Vulnerability Assessment: Team functions as an adversary (Red Team)</td>
</tr>
<tr>
<td>System interoperability and functionality in response to exploited cyber vulnerabilities</td>
<td>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.</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>Cyber kill chain as exercised by the adversary includes the following Activities: Reconnaissance, Weaponization, Delivery, Exploit, Control, Execute, Maintain.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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)
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