Defensive Cyber Operations Testing

Dr. Georgianna “George” Shea
MITRE support to D-DT&E
Who do I support? D- DT&E

Roles and Responsibilities

– Policy, Guidance, and Congressional Reporting.

– Major Program Engagement.

– T&E Workforce

Office of the Secretary of Defense (OSD)

Office of the Undersecretary of Defense for Research and Engineering (OUSD (RE))

Director of Defense Research and Engineering for Advanced Capabilities

Deputy Director, Developmental Test and Evaluation and Prototyping

Director for Developmental Test and Evaluation
DCO Defined

- DCO – Defensive Cyber Operations
- OCO – Offensive Cyber Operations
- DCO- RA – DCO Response Action
- DCO-IDM – DCO Internal Defensive Measures
Cybersecurity T&E Guidance 6 Phases

- Developmental Testing
  - Phase 1 Understanding Requirements
  - Phase 2 Characterize the Cyber-Attack Surface
  - Phase 3 Cooperative Vulnerability Identification (CVI)
  - Phase 4 Adversarial Cybersecurity DT&E (ACD)

- Operational Test
  - Phase 5 Cooperative Vulnerability and Penetration Assessment (CVPA)
  - Phase 6 Adversarial Assessment (AA)
Cybersecurity T&E Process

- **Cybersecurity T&E is necessary and required by policy**
  - Evaluates a system’s mission performance in the presence of cyber threats
  - Informs acquisition decision makers regarding cybersecurity, resilience and survivability

DoDI 5000.02, Enclosure 14 – planning and conducting cyber T&E
DODI 8500.01 Cybersecurity

System Cyber Survivability
System’s ability to Prevent, Mitigate and Recover from cyber events

Security Standards
System meets established standards

Operational Resilience

DODI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations
Phase 1
Understanding Requirements
Example of program cybersecurity requirements:

- Make it cyber secure
- Meet RMF
Actual Requirements

- DODI 8500.01 Cybersecurity, March 2014
  - 3(d) “Cyberspace Defense. Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DoD information networks.

- DODI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations (DODIN) March 2016:
  - DCO Internal Defensive Measures
DoD DCO Requirements:

DoDI 8530.01

EO 13800

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Follow the CSF)
ESM Required Services

- **Implied system requirements**
  - Data repositories
  - Data/Information sharing capabilities
  - Data/Information correlation capabilities
RMF Relationship
## Allocating Responsibilities - Provisioning Cybersecurity Services

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organic</td>
<td>All services self-provisioned</td>
</tr>
<tr>
<td>Single External Provider</td>
<td>Services leveraged from an existing, certified provider</td>
</tr>
<tr>
<td>Multiple External Providers</td>
<td>Services leveraged from multiple existing, certified providers</td>
</tr>
<tr>
<td>Hybrid Mix (Organic &amp; External Provider)</td>
<td>Some services self-provisioned and other services leveraged from an existing, certified provider.</td>
</tr>
</tbody>
</table>

Identify areas of responsibility to include inherited controls to SCA.
<table>
<thead>
<tr>
<th>Step 1: Categorize</th>
<th>DODI 8510.01 supports the Step 6 of RMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2: Select Controls</td>
<td>DODI 8510.01 - “...address security controls that may be satisfied through inheritance”</td>
</tr>
<tr>
<td>Step 3: Implement Controls</td>
<td>DODI 8510.01 inherited security controls, maintained by the providing system</td>
</tr>
<tr>
<td>Step 4: Assess Controls</td>
<td>DODI 8510.01 “...identify all common controls inherited”</td>
</tr>
<tr>
<td>Step 5: Authorize System</td>
<td>DODI 8530.01 Supports the Step 6 of RMF</td>
</tr>
<tr>
<td>Step 6: Monitor</td>
<td></td>
</tr>
</tbody>
</table>
## Sample of Inherited Controls from CSSP

<table>
<thead>
<tr>
<th>ID</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>DCO Common Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>AC-21</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AT-2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AU-6</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CA-1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CA-2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CA-7</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CA-8</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Determine responsibility of controls (organic or external)
NIST 800-137 Approach Information Systems
Continuous Monitoring

DCO Monitoring capability in support of RMF step 6: Continuous Monitoring
Phase 1: Understand DCO Requirements

- Will the system provide a DCO capability or will a provider?

- Is the system designed to enable continuous monitoring (NIST SP 800-137)?

- Do the system requirements account for DCO tools and architectural requirements?
Phase 2
Characterize the Cyber-Attack Surface
Assess Planned Execution

- **People**
  - Experience
  - Offensive cyber mindset
  - Mission understanding
  - Analytical capability

- **Process**
  - Situational Awareness
  - Data Consolidation
  - Effective organizational relationships
  - Repeatable

- **Technology**
  - Tools
  - Automation

Have you established workforce requirements?
Evaluate manning plans and the ability to PMR, across the system.

Have you established process enabling requirements?
Evaluate processes to PMT across the system.

Have you implemented enabling technologies?
Test the technologies ability to PMR across the system.

PPT = People Processes, Technologies
PMR = Prevent, Mitigate, Recover
Assess DCO Capabilities

- **Prevent:**
  - The ability to protect critical mission functions from cyber threats.

- **Mitigate:**
  - The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.

- **Recover:**
  - The resilience to recover from cyber-attacks and prepare mission systems for the next fight.

Have you established prevention capabilities?
Evaluate how PPT enable prevention across the system.

Have you established mitigation capabilities?
Evaluate how PPT enable mitigation across the system.

Have you established recover capabilities?
Evaluate how PPT enable recovery across the system.

PPT = People Processes, Technologies
PMR = Prevent, Mitigate, Recover
Do you have a blind spot?

Testable capabilities during development.

Test:
- Measures of effectiveness
- Measures of performance

Will the (people, process and technologies) effectively (Prevent, Mitigate, and Recover) cyber attacks throughout the system?
Example of Data/Detect/Technologies capabilities across the system to test:

<table>
<thead>
<tr>
<th>Cyber Kill Chain</th>
<th>Perimeter</th>
<th>Internal Network</th>
<th>Endpoint</th>
<th>Application</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon</td>
<td>NIDS, SEIM, firewall, Honeynet...</td>
<td>NIDS, SEIM, firewall, Honeynet...</td>
<td>HIDS, SEIM, host agents, Honeypot, ...</td>
<td>HIDS, SEIM, Application log auditing, Honey file,...</td>
<td>HIDS, SEIM, log auditing, Honey token/Honeyfile,...</td>
</tr>
<tr>
<td>Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Measures of Effectiveness:**
How many intrusions were detected?

**Measures of Performance:**
What sensors are in place?
Phase 2: Attack Surface

- Will activity be detected?

- Does the monitoring capability make the system more vulnerable?

- Has the Incident Response Plan been analyzed/tested? (CTT)

Is there a Defense-In-Depth Strategy being implemented?
Phase 3
Cooperative Vulnerability Identification (CVI)
Testing DCO Capabilities

- **Phase 3 CVI** - verify cybersecurity and resilience requirements, identify vulnerabilities and needed mitigations
  - Cooperative aspects include:
    - Tuning Sensors
    - Baselining
    - Understanding adversary battle plan and mission effects (SOP development for response procedures)
Example of “Tuning” a sensor

Time taken to scan ports

Number of ports scanned

100 ports w/n 1 sec 80 ports w/n 1 min 5 ports w/n 1 min

Thresholds determine the amount of traffic seen.
Example of Baselining

- **Identify what is normal**
  - Is it normal for employee to print at a rate of 10xs more than others?
  - What IPS are expected to be seen within your network?
  - Do system administrative duties line up with identified privilege escalation?

- **How to baseline**
  - Identify what is continually being flagged by sensors and find out why.
  - Tune sensors
  - Identify and record recognized operational events
ESM Assessment ML1 Example
Phase 4
Adversarial Cybersecurity DT&E (ACD)
DCO Test and Evaluation

- **Phase 4 ACD** - tests the system’s cybersecurity and resilience using a mission context in a cyber-contested operating environment.

- **Test:**
  - Prevent, Mitigate, Recover capabilities
  - People, Processes, Technologies
  - Throughout the entire system
Questions?

Contact Information:
Dr. Georgianna Shea
gshea@mitre.org