Department of Defense
Cybersecurity T&E Guidebook
Update and Cyber Table Tops

ITEA Cybersecurity Workshop, 7 March 2018
Sarah Standard, DASD(DT&E)
Cybersecurity/Interoperability Technical Director
Requirements, Policy and Guidance BLUF

• Joint Staff, J6 System Survivability KPP including a Cyber Survivability Endorsement updated January 2017

• DoDI 5000.02 added Enclosure 14 updated January 2017

• DOT&E Cybersecurity OT&E Memo August 2014 now under review

• DoD Cybersecurity T&E Guidebook update in progress

• OSD Cyber Table Tops (CTTs) Guidebook in development
DoD Cybersecurity T&E Guidebook

- Version 1.0 – July 2015
- Version 2.0 published February 2018
- Describes each phase, inputs, outputs, tasks
- Addresses RMF integration
- Update includes new appendices
  - Phase 1-6 Quick Look
  - Cyber Threat Assessments (FOUO document)
  - Tailoring the Phases
  - Considerations for Cybersecurity Measures (FOUO document)
    - SS KPP and Cyber Survivability Attributes
  - Cybersecurity Test Considerations for Non-IP Systems (FOUO document)
  - Mission-Based Cyber Risk Assessments (CTTs) (FOUO document)
  - Cybersecurity T&E Contract Language Considerations
  - Software Assurance Testing
- FOUO appendices will be published separately
Update Objectives

- Align with DODI 5000.02 Enclosure 14 release
  - Cybersecurity In The Defense Acquisition System
- Promote mission-impact based analysis and assessment methods
  - Data driven
- Encourage tighter integration with functional T&E
  - Assessment of cyber resilience within mission system context
- Promote practitioner best practices
  - Include “from the trenches” test activities – what works, what doesn’t
  - What tests and data from DT can inform Protect, Detect, React, Restore and improve adversarial assessment results during OT
  - Offer sanitized, real world examples whenever possible
- Document a distinct value proposition for cyber DT&E
  - Short introductory summary in Chapter 3 – overview of phases and concepts
  - “Role of Cybersecurity Developmental Testing”
The goal of cybersecurity DT&E is to identify issues before MS C that are related to resilience of military capabilities from cyber threats. Early discovery of system vulnerabilities can facilitate remediation and reduce impact on cost, schedule, and performance.

Operational cybersecurity testing supports the evaluation system effectiveness and suitability (and survivability).
• Beginning in November 2017, Guidebook 2.0 was distributed for review by Services and Components

• 39 reviewers received the draft for review, most submitted comments, many shared with others
  – In the end, 37 individuals submitted comments

• 389 comments received
  – High quality, thoughtful comments
  – All comments were reviewed and adjudicated by the Guidebook Core Team
  – 80% of comments were accepted or partially accepted
  – Rejected comments
    – Service Specific: Comment not incorporated because it was not applicable to all Services
    – Overly Prescriptive: Comment not incorporated because it provided too much detail on “How” to perform a task or limited the flexibility any Service-specific methods
    – Inconsistent with Intent: Comment not incorporated because it was not applicable to the purpose of the Guidebook or was out of scope (e.g., not T&E specific)
    – Clarified Intent: Comment not incorporated but the applicable text was modified to clarify the misunderstanding that led to the comment
Comments Recap

Air Force: 59
Army: 73
Navy: 149
USMC: 6
DIA: 12
DOT&E: 37
OSD: 41
DoD CIO: 12

7 N/A Service Specific
10 N/A Overly Prescriptive
52 N/A Inconsistent with GB Intent

16 Comments Partially Accepted
298 Comments Accepted
389 Comments
6 N/A Clarified Intent
CYBER TABLE TOPS
Cyber Table Tops (CTTs)

- One of many mission-based cyber risk assessment methodologies aligned to National Institute of Standards (NIST) guidance for conducting information system risk assessments.
Some programs find it difficult and confusing to negotiate the policy and processes for developing their requirements and strategy for cyber T&E.

The Cyber Table Top (CTT) Wargame Exercise is one way to identify credible vulnerabilities and develop actionable requirements that can be used to design efficient T&E:

- Need to ‘right size’ testing
- To identify what’s most important

CTTs are mission based risk assessments that align to the NIST 800-30 Risk Assessment Guide and can inform each step of the Risk Management Framework in addition to cyber T&E.

You can’t test to 100%:
- What are the significant vulnerabilities?
- What are the acceptable risks?
- How do you develop a plan?
Cyber Table Top (CTT): What, Why?

• **What is a CTT?**
  – Low technology, low cost, intellectually intensive exercise to introduce and explore the effects of cyber offensive operations on the capability of a System, SoS or FoS to execute a mission

• **Why is it used?**
  – **Identify** potential threat vectors, risks associated with threat vectors, and potential threats from boundary systems
  – **Categorize** cyber threat consequence by likelihood and impact within the assessed mission context
  – **Inform** mitigations analysis, engineering, testing and design activities

• **What does it produce?**
  – Cybersecurity risk matrices based on posited mission effects
  – Initial categorization of families of threats into three categories
    – Threats that **must** be mitigated to assure mission performance
    – Threats that require additional analysis prior to developing mitigation strategies
    – Threats that are assessed to be low risk/impact and may be accepted
  – Recommendations for actionable steps to increase resistant and resilience to cyber attacks

Candidate cyber attacks are logically plausible based on technical data provided; they are NOT proven-to-work, tested, hands-on attacks
CTT: How?

• Seminar of two teams of SMEs with opposing missions and a Leadership Team

• **Operational Team Mission**: Step through how to use the system within a mission scenario

• **Opposing Forces (OPFOR) Team Mission**: Step through cyber attack missions

• **Control Team Mission**: Leadership: create, conduct, analyze, and out brief the CTT

• **Operational and OPFOR Teams** collaborate and work through the assumptions, consequences, workarounds to successful threat attacks and determine how that relates to mission success

• Data collected during CTT feeds into post exercise analysis, cybersecurity risk matrices, and next step recommendations
Purpose of the CTT

- Provide PMs, engineers and testers with actionable information on high priority/high impact cyber threats

- Identify specific high-value follow-on analysis and testing to verify and quantify actual risks

- Actionable information
  - Potential vulnerabilities
  - Demonstrated means of exploitation
  - Assessment of the mission impacts

- Prioritize
  - Attack surfaces that are most exploitable
  - Attack methods that, if successful, could be the most harmful to mission

Disciplined approach to bridge the gap between the Information Technology and Warfighter viewpoints
CTT Benefits

• **Pragmatic, affordable method** to implement elements of the cybersecurity T&E phases

• **Generate actionable information** on high priority/high mission impact cyber threats

• **Define specific high-value follow-on analysis and testing** to verify and quantify actual risks

• Provide the Program Manager’s engineering and test team opportunities for risk reduction throughout the life cycle

• **Reduce the likelihood and cost** of cyber vulnerability discovery during operational testing and deployment

• **Socialize the concepts of cybersecurity** for program office and operators, bridging the gaps between systems engineering, testing, and operating
Approximate average execution time (varies depending on team experience and scope of evaluation)

- Exercise Preparation: 30 – 60 days
- Exercise Execution: 3-5 days
- Post Exercise Analysis: 30 – 90 days
- Reporting: Varies

**CTT Process**

**OSD CTT Guidebook in Development**

Operational Mission & Scenario Development

Logistics Personnel Planning

Cyber Mission Development & Reconnaissance

Control Team

Exercise Preparation ➔ Exercise Execution ➔ Post Exercise Analysis ➔ Reporting

- Team Mission Development and Execution
- Data Collection and Review
- Likelihood and Impact Assessment
- Cybersecurity Risk Matrix

Control/Analysis Team

Operational Team ➔ Cyber OPFOR Team

Must Test ➔ Accept Risk ➔ Further Analysis ➔ Mitigation

LIKELIHOOD Matrix

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>5</td>
<td>Very Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

IMPACT (K)

1 2 3 4 5
Examples of Realized Benefits of the CTT

- Identified multiple cyber threats that were tested and analyzed in Developmental and Operational Test (DT/OT)
- Identified a significant cyber threat one year before it was identified as a high-priority “in the wild” threat impacting numerous systems
- Produced a risk assessment consistent with a Risk Assessment Report (RAR) – at a much lower cost and clearer mission impact!
- Outbrief of CTT results to PM resulted in directive to execute tests and support briefings to DOT&E
- On average, CTTs document 60 attacks where at least 25% are high or very high risk
Questions

sarah.m.standard.civ@mail.mil
571-372-2778