Office of the Director for Developmental Test, Evaluation, and Assessments (D,DTE&A)

Cyber Testing

June 16, 2021

Ms. Sarah Standard

Cybersecurity/Interoperability Technical Director

Distribution Statement A:
Approved for public release, distribution unlimited

Agenda

- Cyber Test and Evaluation (T&E) Challenges and Opportunities
- Ongoing and Planned Initiatives in Developmental Test, Evaluation and Assessments (DTE&A) for Cyber T&E
- Cyber T&E in 5+ Years
- Industry Evolution

Focus is on Cyber Developmental Test and Evaluation (DT&E)

Cyber Test and Evaluation Challenges – History

- **Presidential Directive defined "cybersecurity" – DoD replaces "IA" with "Cybersecurity" – DoDI 8500.01**
  - Requires all DoDI Information Technology to meet 10 "requirements" including in the areas of:
    1. Risk Management: DoD transitioned policy from the information assurance (IA) certification and accreditation checklist process to Risk Management Framework (RMF) Assessment and Authorization (A&A)
    2. Operational Resilience - The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions
    3. Integration and Interoperability – manage interface risk

Results?

- **DoD published the "shift left" guidance, Guidebooks for RMF, cybersecurity T&E (2015)**
- **Getting an Authorization to Operate (ATO) under RMF became the focus for Developmental Test and Evaluation (DT&E) contracts – and remains so today**
  - Vulnerability scanning
  - Apply Security Technical Implementation Guides
- **In Operational T&E, Red Teams successfully demonstrate systems with ATOs are vulnerable, typically to low level threat tactics**

- **What went wrong?**

Distribution Statement A:

Approved for public release, distribution unlimited

Cultural Changes Lagged

- **Intentions good**
- **Execution and resources continue to be poor or too late**
- **Education and awareness all RMF focused**
  - RMF is a separate, parallel effort
  - "Program cyber person"
  - RMF is sufficient
- **Threat and mission have a back seat to the ATO**
  - Not elevating cyberspace as an operating environment for every system
  - Common Enterprise IT protection checklist mindset versus operational resilience needs – think like a hacker
- **Contracts focused on RMF for cyber DT&E**

Distribution Statement A:
Approved for public release, distribution unlimited

Top 10 Program Excuses for Dodging Cyber Testing…

The 11 top 10 excuses gathered from the Operational Test Agencies:

1. The DOT&E Memo is only a recommendation for Programs under DOT&E Oversight. We are not under DOT&E Oversight so we don't have to comply with the memo.
2. The cybersecurity for my program is inherited
3. No true governance behind Cybersecurity DT&E - It's only a guidebook
4. We have done enough testing through RMF or we already have an ATO. RMF covers the DT test requirements
5. FedRAMP should cover all of our testing requirements
6. The coordination process to get the system tested is too long and we need to field the system
7. This is not in our TEMP so we don't have to do it
8. We don't have a TEMP so we don't have to do cyber DT/OT.
9. You're the tester, you can't make up requirements for the program
10. The CSE does not apply to our program even though we have joint users across the services and agencies. We are just a business system.
11. This testing is not covered in our RFP. Therefore, we cannot conduct testing.

Collected ~2017-2018//Courtesy of DOT&E

Along the Way…

- **Requirements: Joint Staff published update to the required System Survivability Key Performance Parameter (SS KPP) to include a mandatory Cyber Survivability Endorsement (CSE)**
- **Strengths**
  - CSE Implementation Guide (yet another guidebook)
  - Focus on Prevent Mitigate and Recover (instead of NIST Protect, Detect, React, Recover) to align to SS KPP pillars
  - Mission and threat relevance
  - Ten Tailorable Cyber Survivability Attributes (CSAs)
- **Weaknesses**
  - Only "joint" programs or "joint interest" programs required to go through the Joint Staff requirements process
  - Coupled to the RMF controls

Distribution Statement A:

Approved for public release, distribution unlimited

Cyber Test and Evaluation Today

- **DoD cyber DT&E capability improvements**
  - Cross-service collaboration and sharing; workforce standards
  - Cyber range expansion (capability, capacity, demand)
  - Integrated Cyber Test Teams with Contractor
  - Government DT&E integrated with government OT&E
  - 2020: Version 2.1 of the DoD Cybersecurity T&E Guidebook published
  - “RMF is necessary, but not sufficient”
  - Mission-based Cyber Risk Assessments (MBCRAs) are required
    - Cyber Table Top, Mission Risk Assessment Process for Cyber
    - Essential for scoping test, attack surface and criticality analysis
    - Helps program, helps tester, helps operational user, helps developer
    - Improves overall engineering – merging with other disciplines in program protection
- **Service requirements moving toward requiring CSE for all programs and “cyber resilience”**

Distribution Statement A:
Approved for public release, distribution unlimited

Cyber Testing Challenges Today

- **Programs do not (universally)**
  - Address requirements beyond RMF, even with CSAs
    - Still no operational resilience requirements
  - Require recurring cyber T&E by contractors
  - Require mitigations by contractors beyond RMF non compliance (eMASS)
  - Perform or resource adequate government cyber DT&E
  - Involve test organizations early enough
- **Overwhelming amount of policy and guidance lacking consistency and clarity with heavy RMF emphasis**
  - Lags guidance
- **OT&E routinely finds DoD systems to be various degrees of "cyber secure", but usually not very secure or very enduring**

Distribution Statement A:
Approved for public release, distribution unlimited

Ongoing Challenges in Today's Landscape

- **Culture change still lagging**
  - Acknowledge the insider threat is valid at any point in the lifecycle
  - Cyberspace is a warfare environment all the time (during system development and post fielding)
  - Keeping up with cyber test responsibilities (commercial cloud, DevSecOps, Non-Developmental Item)
- **Legacy programs don't update requirements to address threat**
- **Repurpose old program documents, copy and paste**
  - Not devoting the necessary up front critical thinking
- **Engineering standards for resilience and test not mature**
  - What is "resilience," what is "survivability?"
  - How to test and measure resilience, survivability?
  - What is my threat?
  - Can't test on that test asset!

Distribution Statement A:
Approved for public release, distribution unlimited

Other Challenges in Today's Landscape

- **No sustainment cyber T&E planned (or required)**
- **Intelligence community is lagging on ability to articulate cyber threat – sharing those details with industry is hard**
  - Active efforts ongoing to improve cyber intel support to acquisition
- **Rapid acquisition – go fast, skimp on test**
- **Risks are not well understood - Think like a hacker!**
  - Development and test environments (at every level in the supply chain) – hardware, software, firmware, networks
  - Development and test processes (code reuse, open source, COTS)
  - Development and test tools
  - Hidden dependencies (e.g. infrastructure, water, power, HVAC, Internet of Things)
  - Commercial clouds

Distribution Statement A:
Approved for public release, distribution unlimited

What's needed?

- **Addressing these challenges requires a robust cybersecurity process**
  - NEED: Clarity in acquisition policy
  - IMPROVE: Thorough cyber and test requirements provided to contractor, informed by government cyber testers
  - IMPROVE: Engineering resilience into the system informed by government cyber testers – contractor innovation
  - IMPROVE: Early and thorough DT&E using a threat tactics and mission capabilities informed approach – SHIFT LEFT
  - IMPROVE: Continuous feedback to the development engineers for action – test, fix, re-test
  - CONTINUE: Operational testing that informs acquisition and employment decisions

Distribution Statement A:
Approved for public release, distribution unlimited

Now and Future: Ongoing Initiatives in DTE&A

- **Shift Left in Cyber (SLiC)**
  - Engage cyber analysts and testers with programs early – measure impact
  - Focus on developer/contractor testing, to include developer and test environment, processes, tools (supply chain)
  - Multiple DT&E events, not singular after system is complete, not just scans and control assessment
  - Push for DT&E results to inform ATOs

- **Ongoing collaboration**
  - Cyber Developmental Test Cross-Service Working Group
  - Cyber Survivability Endorsement Working Group (cross-OSD)
  - Multiple "dot-connecting" for programs, test organizations, OSD and Service
  - Teaming: Federally Funded Research and Development Centers, University Affiliated Research Centers, Systems Engineering Research Center

Distribution Statement A:
Approved for public release, distribution unlimited

Other Ongoing Initiatives in DTE&A

- **PWN2HONE – private bug bounty on an acquisition program using only DoD cyber testers**
  - Increase diverse cyber DT&E on the component/sub system
  - Expand DoD cyber tester knowledge, skills, abilities
- **Ontology for Attacks in Cyber Risk Assessments (OACRA)**
  - Map cyber attacks documented in prior Cyber Risk Assessments (CRA) to a common framework
  - Enable efficient information sharing and machine reasoning
- **Policy and Guidance – mission-risk, threat-focused, continuum of cyber T&E, resilience engineering**

Distribution Statement A:
Approved for public release, distribution unlimited

In Work: Joint DT/OT Cyber T&E Memo

- **Approach: A dual-signature memorandum replacing the existing single-signature "cybersecurity procedures" memorandum to update and refine prior guidance**
- **Themes:**
  - Threat and mission-informed early, recurring activities defined by program cadence
  - Share more: closer integration of contractor/government, as well as DT/OT
  - Expand data collection and analysis to include software assurance, system recovery, supply chain risks, security of developmental environments, cloud and other specialized testing
  - Align memo and Cybersecurity T&E Guidebook (what-to-do guidance matched with how-to-do-it resources)
- **Support Adaptive Acquisition Framework and DoDI 5000 policies**

Promote a "shift left" mindset, perform testing early and often!

In Work: Cybersecurity T&E Guidebook v3

- Provide the “how to” for gathering required data described in the Joint DT/OT memo
- Promote early integrated cyber T&E
- Support varied cyber test cadences under the new Adaptive Acquisition Framework
- Easier to use web-based format

- Improve guidance for
  - Cyber/electronic warfare testing
  - Cyber Supply Chain Risk T&E
  - Automated cyber T&E
  - Planning and documentation
  - Measuring resilience and survivability
  - Testing recover and response in DT&E
  - Testing maintenance processes in DT&E
  - Evaluating and reporting
  - Sustainment cyber T&E

Distribution Statement A:
Approved for public release, distribution unlimited

Now and Future: Mindset Change

- **More cyber T&E, not less**
  - Integrated testing essential for rapid programs
  - Early planning critical to defining the cadence and scope
  - Test "ilities" in contested cyber environment
- **Speed can improve resilience and survivability**
  - Not a given! DevOps versus DevecOps – Major paradigm shifts needed – critical thinking and planning
- **Commercial clouds are not necessarily secure – shared security roles – it is usually your fault, not the cloud provider's**
  - Cyber DT&E in a twin environment with twin interface representation
- **Zero trust architectures**
  - Don't trust, always verify

Distribution Statement A:
Approved for public release, distribution unlimited

Cyber Test and Evaluation in 5+ Years

- **Automated cyber T&E moving from software to operational technology**
  - Incorporating more modeling and simulation as well as Artificial Intelligence/Machine Learning (AI/ML)
  - Digital Twins, Model Based Systems Engineering
  - Software modeling (test like you fight, before you build)
- **Cyber T&E techniques for AI/ML enabled systems**
- **Better understanding and awareness of the full attackable surface**
  - Development and test environments, processes (human roles), and tools
  - Infrastructure and interface dependencies
- **Cyber T&E that addresses complex attacks by incorporating interrelated capabilities (EW, IO, deception)**

Distribution Statement A:
Approved for public release, distribution unlimited

Cyber Test and Evaluation in 5+ Years

- **Model-Based Systems Engineering and Digital Engineering**
  - Mission capability models that align to system providing capability models – capability based cyber T&E (“ilities”)
  - Need a single cyber schema to define resilience, survivability
  - Cyber tools perform analytics and cyber testing of the model
- **Using simulated interfacing and interdependent systems to fully examine the attack paths and vulnerabilities with digital twins**
  - Multi-use testing environment for “ilties”
- **Increased contractual liability and regulatory requirements**
- **Cyber readiness level definitions with readiness progression akin to Technology Readiness Levels**

What DoD Needs to Improve

- **Request for Proposal Language for Cyber DT&E**
  - Sub-component, component, sub system – threat and mission informed
  - Cyber Supply Chain Risk T&E
  - Mitigation/fixes
  - Contractor demonstrates cyber resilience and survivability performance
  - Product acceptance cyber T&E
- **Integrated contractor/government cyber DT&E**
  - Mission impact informed; intelligence informed (but not dependent)
  - Tool and threat sharing

Distribution Statement A:
Approved for public release, distribution unlimited

Industry Evolution

- **Submit clarifying questions to request for proposals**
  - Help DoD provide clearer resilience, survivability, and cyber T&E requirements
- **Scrutinize your supply chain, development and test environment, processes, and tools**
- **Educate across your organizations – Think Like a Hacker**
- **Build and engineer for resilient proof of concepts – test "ilities"**
  - Don't design and engineer re-using components or using new components that have never been proven/designed to be DoD-mission resilient
- **Seek to integrate the government cyber T&E organizations from the start of a contract**
- **Help pursuit of standard cyber schemas in model-based systems engineering**

Distribution Statement A:
Approved for public release, distribution unlimited

Q &
A

sarah.m.standard.civ@mail.mi
l

Resources

DoD Cybersecurity T&E Guidebook, v2.1

- https://www.dote.osd.mil/T-E-Enterprise/ (no CAC)
- Version 3 under development; Estimate 11/30/2021

DoD Cybersecurity T&E Guidebook For Official Use Only Appendices v2

- https://intelshare.intelink.gov/sites/resp/CTT/ (CAC)
- Located in the DoD Cybersecurity Test and Evaluation Guidance folder under Shared Documents. Version 3 will change to CUI content; under development

DoD Cybersecurity T&E for Commercial Cloud – Addendum to the DoD Cybersecurity T&E Guidebook

- https://www.dote.osd.mil/T-E-Enterprise/ (no CAC)

DoD Cyber Table Top Guidebook

- https://intelshare.intelink.gov/sites/resp/CTT/ (CAC)
- Located in the Mission Based Cyber Risk Assessment Methodologies folder under Shared Documents
- Update to Version 2 in progress

Cyber Developmental Test Intelink/CTT site:

- https://intelshare.intelink.gov/sites/resp/CTT/ (CAC)
- Includes calendar of events, past CTTs, CTT Facilitator list, CTT templates, CTT facilitator folders, discussion board, and survey, Mission-Based Cyber Risk Assessments (MBCRAs) Comparative Study, Other MBCRAs

DoD Centralized Cyber Capabilities Directory (C3D)

- https://rdte.services.nres.navy.mil/C3D (CAC)
- A web application to serve programs and the cybersecurity testing community as a searchable rolodex of cyber test tools, facilities, and service providers.