Addressing the Needs of Cybersecurity T&E

Briefing for the ITEA Test Instrumentation Workshop

May 12, 2016

Chip Ferguson

TRMC, Deputy to the Executive Agent, Cyber T&E Ranges

Agenda

- **Workshop Impressions So Far**
- **What's New with JMETC**
  - JMETC Multiple Independent Levels of Security Network (JMN)
- **Cyber Security Table Top**
  - Advantages of conducting a Cybersecurity Table Top exercise as a method to identify vulnerabilities to be used in developing a Cybersecurity T&E plan.
- **Newly appointed Executive Agent (EA) for T&E Cyber Ranges**
  - Vision of the EA
  - Congressional direction
  - Near-term Activities to begin achievement of that vision
  - Relationship between the EAs for T&E Cyber Ranges and Training Cyber Ranges
  - Participation by the Services and Agencies

What's New With JMETC

JMETC Managed Distributed Testing Infrastructures:

JMETC SECRET Network (JSN)

Regional Service Delivery Points (RSDPs)

JMETC MILS Network (JMN)

JMETC SECRET Network (JSN)

- Objective is to provide ***persistent connectivity*** ***on an OPEN network***
  - Standing IA Agreements
  - Daily full mesh, end-to-end network characterization ensure optimized performance
  - On demand usage with little to no coordination necessary
- Operates at SECRET Collateral
  - Leverages SECRET Defense Research & Engineering Network (SDREN) for connectivity
- Primary support to NR-KPP, Systems and System-of-Systems Integration and Interoperability (Shift Left), across the acquisition life cycle.
- Limitation
  - Does not support Cyber and Coalition requirements
  - Does not support higher security classifications

JMETC SECRET Network (JSN)

Functional Sites: 74
New Sites Planned: 8
Connection Points to Other Networks: 5

- Leverages the SECRET Defense Research and Engineering Network (SDREN) for connectivity
- Operates only at the SECRET classification
- Continuous monitoring, troubleshooting, and optimization of the end-to-end network infrastructure
- Capable of supporting numerous simultaneous test events

Keyport NUWC

Site in Alaska
Ft. Greely: CRTC

Edwards (2): Ridley
412th EWG IFAST
China Lake (3): F/A-18, IBAR, TSPIL
Point Mugu (3): ITEC, AEA, EW CyCon
Camp Pendleton: MCTSSA
Corona: NSWC
Point Loma :
SSC-PAC 59140
SSC-PAC CTB LMMT
W. Interconnect Rtr.
Rancho Bernardo
NGC Triton

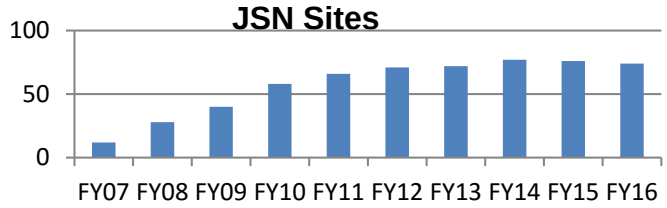
Site in Hawaii
MHPCC

Dugway Proving Ground
USSTRATCOM
Crane (2): NSWC RDT&E, NTN Lab
WPAFB: SIMAF
Rome NY AFRL
Pittsfield GD LCS
Newport NUWC
Moorestown (2): CSEDS, CPTS
Aberdeen: ATC-STE, ARL
Dahlgren: (3) IWSL, DOC, ICSTF
Rapid-SIL/C2
Pax River: (9) E2C, E2D, MCL, ACETEF, SAIL, ATR, E-2C SIL, UASIL, MFS
EP-3
JMETC SYSCON
East Interconnect Rtr.
JS J8 DDC4 C4AD
Langley TDLITC
Dam Neck CDSA
Wallops Island SCSC
Newport News NGC VASCIC
McLean MITRE NSEL
Metro Park JMETC / TENA SDA Lab
Richmond NRO CTE

Redstone (10): SMDC
RTC: DTCC, DISTL
SED: Patriot, THAAD, FAAD, GSIL, JLENS, MUSE, C-RAM
AMRDEC

Kirtland AFB DMOC
Tinker AFB AWACS
Raytheon Tucson
Yuma PG
Ft. Sill (2): FSED, SMART Lab
WSMR IRCC
Greenville Rivet Joint
GTRI
Charleston (2): SSC Data Ctr
MEF-MEU
Ft Huachuca: (4) JITC, JTDL, CMIS, JTRS
Ft Hood (2): CTSF, TTEC
Eglin AFB (4): AOC, DTF, GWEF, KHILS
LMCO Global Vision Network
Melbourne NGC JSTARS

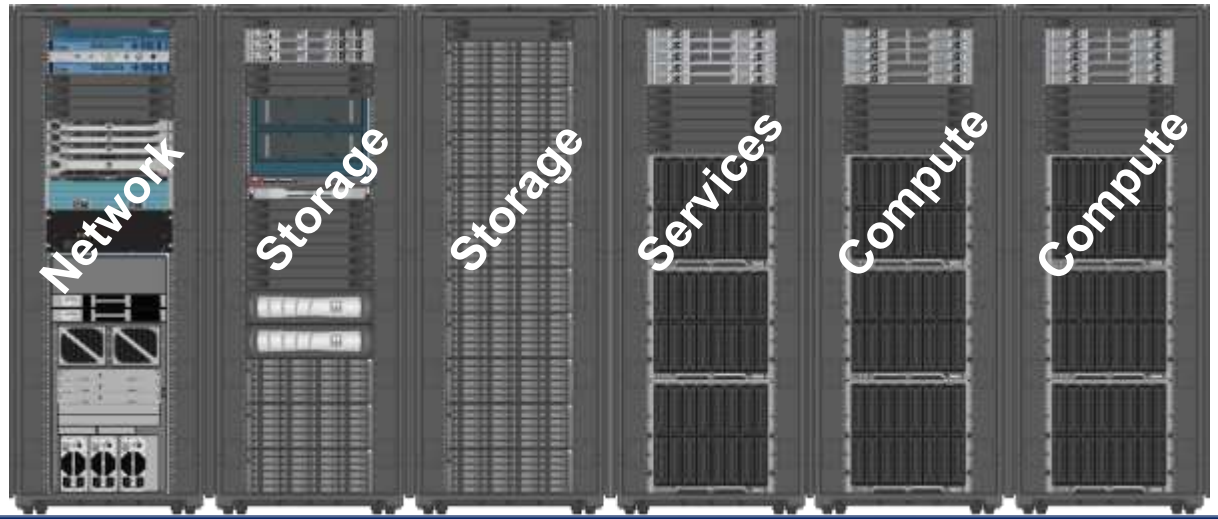
Army
Air Force
Navy
Marines
Joint
Industry



As of 25 Apr 2016

Regional Service Delivery Points (RSDPs)

- Provides enterprise resources focused on generation of virtualized representative network environments
  - Cloud based computational and storage assets to host virtualized representations of Red, Blue, and Gray environments – can host 1000's of high fidelity virtual representations
  - Platform for tools and services (e.g., planning, traffic generation, instrumentation, visualization, integrated event management, collaboration)
  - Supports conventional types of testing (e.g., scalability, performance testing, etc.) as well as cybersecurity testing



Current status: 3 functional with 2 more planned

Regional Service Delivery Points (RSDPs) Capability Overview

- Each is capable of supporting numerous events and varying classifications concurrently
- Also serves as a platform for tools and services (e.g., traffic generation, instrumentation, visualization, integrated event management, collaboration)
- Modular architecture can be expanded or reconfigured to meet evolving requirements
- Geographically dispersed to minimize latency and maximize usability
- Blade architectures implementation is more feasible but has limitations
- Hosted on the JMETC MILS Network (JMN)

JMETC MILS Network (JMN)

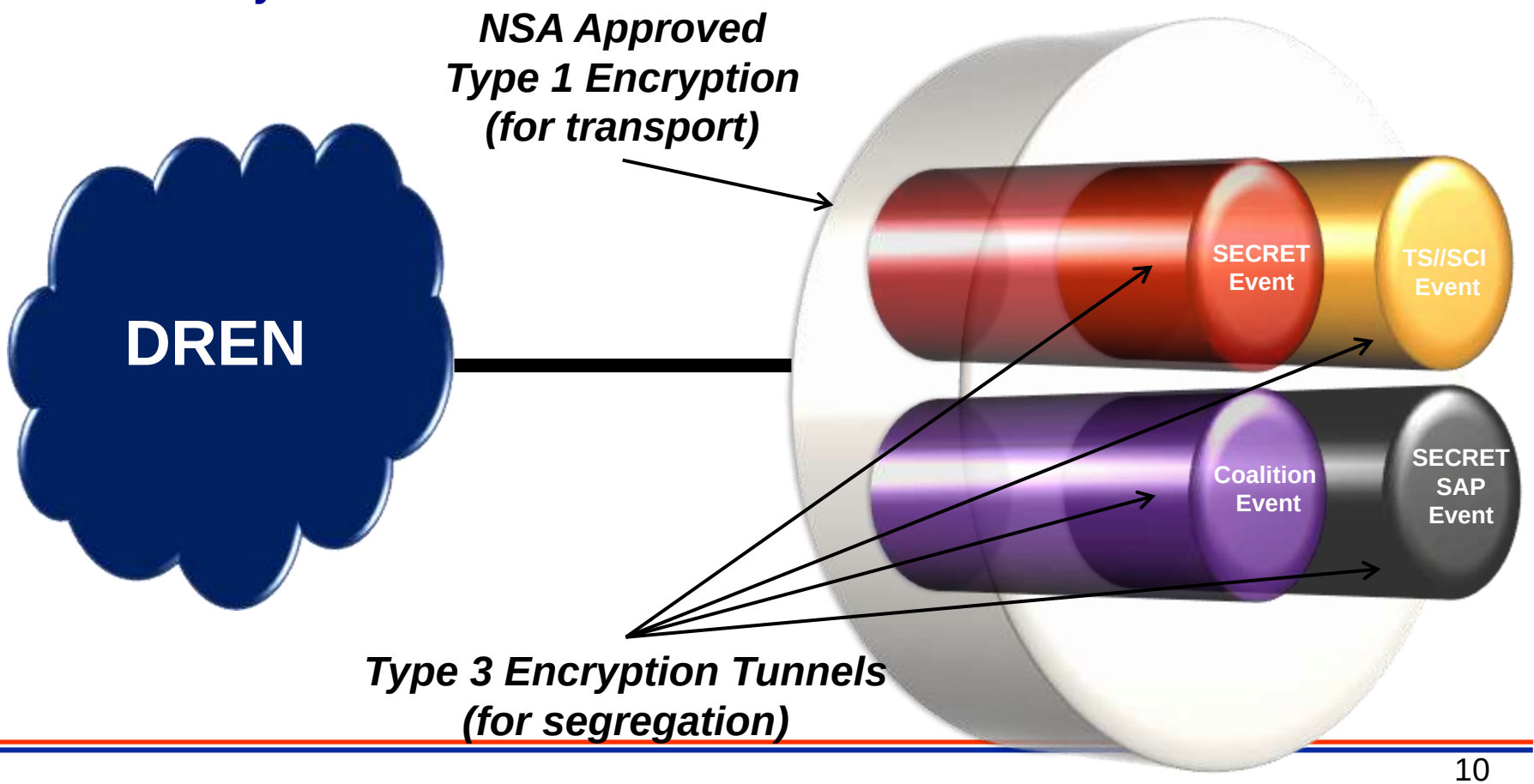
- Objective is to provide 1) access to ***enterprise resources, tools and services*** at ***higher classifications*** and 2) ***isolated distributed testbeds*** ***on a CLOSED network*** to meet growing interoperability and Cyber T&E requirements
  - Accredited by DIA to operate up to TS//SCI/SAP/SAR (included NSA Red Team assessment)

- Employs Multiple Independent Levels of Security (MILS) architecture
  - Allows for segregation of data streams by protocol, system, event, COI, etc.
  - Ability to create “sandboxes” for Cyber events
  - Capable of supporting multiple simultaneous events at multiple classifications concurrently
  - Utilizes Defense Research & Engineering Network (DREN) for unclassified network transport

- Limitations
  - Requires security agreements for each event (valid up to 1yr)
  - Some tools and services may not be available unless JMN support personnel are “read on”

Multiple Independent Levels of Security (MILS) Architecture

- Use unique Type-1 Encryption Key for bulk transport over DREN
- Use Type-3 Encryption to segregate environments and users
- Each site can support multiple classifications and environments concurrently



Cyber Table Top

Cybersecurity Test Requirements Challenge

- **A program says, "I need to do cybersecurity testing. What do I need to do?"**
  - What are the vulnerabilities?
  - T&E budgets cannot realistically sustain testing every communications pathway
- **Answer, execute a Cybersecurity Table Top**
  - A mission based approach to analyzing the risk of cyber threat vulnerabilities
  - Provide a pragmatic affordable means to implement elements of the DoD six-phase Cybersecurity process for DT&E and DOT&E
  - 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

Cybersecurity Test Requirements Challenge

- **Two Opposing Teams and a Control Team**
  - Operation Team (Blue): Develop and step through a mission in response to the mission orders provided by the Control Team. In short, they will "execute" an operationally realistic mission during the table top wargame.
  - Opposing Forces (Red): Examine potential threat vectors and cyber-attack methods applicable for each mission order assigned by the Control Team.
  - Controllers Team (White): Drives the CTT from concept to final report. Responsible for the CTT mission and mission scenario with a focus on operational relevance and mission effectiveness.

The CTT wargame is not to fight with moves and counter moves but to identify cyber vulnerabilities.

Navy P-8 Increment 3 Using CTT Methodology

- **Naval Post Graduate School conducted the Red Recon**
  - Provided the results to the opposing forces on the first day of the CTT
- **Success of the CTT is highly dependent on participation from multi-disciplinary teams, each with a mission to execute**
- **P-8 found the CTT to be a viable exercise to determine**
  - Possible threat vectors
  - Risks associated with Threat Vectors
  - Potential threats from boundary systems
- **CTT is driving immediate actionable next steps for the P-8 Program and will continue to be refined for right size testing**
  - One step in a comprehensive cybersecurity test strategy

More details in the NAVAIR Cyber Table Top Guidebook (www.jmetc.org) and Sept article in ITEA Journal

Newly Appointed Cyber T&E Range Executive Agent

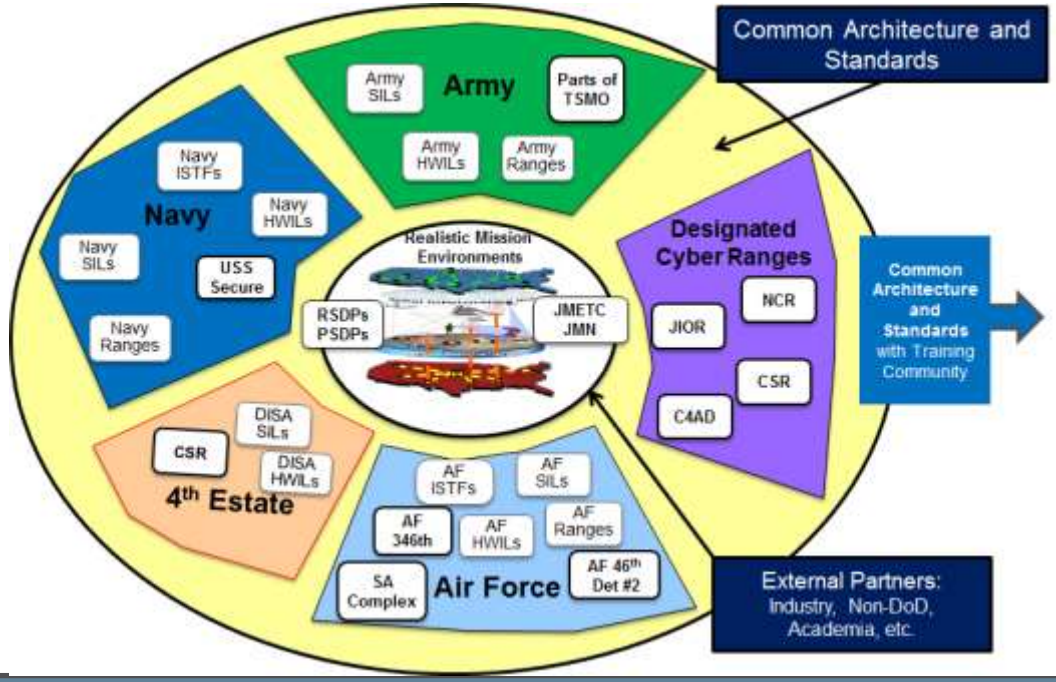
2015 NDAA requires Executive Agent (EA) for Cyber Test to:

1) **Development of the Biennial Integrated Plan** which includes:
   a. Maintaining comprehensive list of test capabilities (DoD and non-DoD)
   b. Organizing and managing designated test capabilities
      - Establish priorities
      - Develop and Enforce standards
      - Guidance to integrate designated capabilities
      - Finding cost reductions
      - Add or consolidate cyber test capabilities
      - Enhance quality and expertise of workforce
      - Coordinate with interagency and industry partners
   c. Define architectures to:
      - Meet evolving needs
      - Coordinate with interagency and industry partners
      - Allows integrated closed loop and EW
      - Supports S&T, R&D, DT&E, OT&E, etc.
      - Connectivity to existing ranges

2) Certify cyber test infrastructure

3) Generate requirements and standards for cyber security test infrastructure.

Vision: Create the Cyber Test and Evaluation Infrastructure (CT&EI)



The CT&EI is composed of existing non-kinetic Cyber test capabilities integrated with representations of kinetic and C2 systems (e.g., hardware-in-the-loop (HWIL) facilities, system integration labs (SILs), and software-in-the-loop (SWIL) facilities) via network connectivity, enabling testing those systems in a realistic combat, including cyber and interoperability, environment. We have to integrate these existing facilities in a cyber environment with low risk of damage.

3 Categories within the CT&EI

- **Designated Cyber Ranges**
  - NCR, JIOR, CSR, C4AD
  - Possibly others at some date
- **Aligned Capabilities**
  - Compliance with architecture and standards
  - Partnership with the EA for Cyber Test Ranges
  - Subject to Budget certification
  - Make category desirable for more nodes to join
- **Occasionally Connected Capabilities**
  - Can connect to the Aligned CT&EI on a case-by-case basis
  - Minor players, Academic, Non-Sponsored Industry, Coalition, etc

Summary

- Great Test Instrumentation Workshop
  - Thanks for inviting me
- JMETC is changing to meet customer requirements
- The T&E Cyber Range EA is Up and Running

Points of Contact

Deputy to the Cyber T&E Range EA:	**Chip Ferguson** **benard.b.ferguson.civ@mail.mil** **571-372-2697**
JMETC Program Manager:	**AJ Pathmanathan** **arjuna.pathmanathan.civ@mail.mil** **571-372-2702**
JMETC Lead Operations Planning:	**Marty Arnwine** **martemas.arnwine.civ@mail.mil** **571-372-2701**

www.jmetc.org

BACK UP

CTT Exercise Overview2