Enhancing the Infrastructure for Interoperability, Cybersecurity, and Distributed Test & Evaluation

2016 ITEA Cybersecurity Workshop

By

Chip Ferguson

Deputy Director, Interoperability, Cyber, and Distributed Test Capability

Test Resource Management Center (TRMC)

Agenda

- Mission
- JMETC Components
  - JMETC Secret Network
  - Regional Service Delivery Points
  - JMETC MILS Network
- Challenges
- Summary

The JMETC Mission

JMETC provides the ***persistent and robust infrastructure (network, integration software, tools, reuse repository)*** **and** ***technical expertise*** to integrate Live, Virtual, and Constructive systems for test and evaluation in Joint Systems-of-Systems and Cyber environments

You Worry About Your Test…
JMETC Worries About the Infrastructure

Three Components of the JMETC Managed Infrastructure:

JMETC SECRET Network (JSN)

Regional Service Delivery Points (RSDPs)

JMETC Multiple Independent Levels of Security (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: 79
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, EA-6B. EW CyCon
Camp Pendleton: MCTSSA
Corona: NSWC
Palmdale, Triton
Point Loma:
SSC-PAC 59140
SSC-PAC CTB LMMT
W. Interconnect Rtr.
Rancho Bernardo
NGC Triton

Sites in Hawaii
PMRF: Bldg 105
MHPCC

Dugway Proving Ground
USSTRATCOM
Crane (2): NSWC RDT&E, NTN Lab
WPAFB: SIMAF
Rome NY AFRL
Newport NUWC
Moorestown: CSEDS
Moorestown: CPTS

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
Ft. Bliss MCC
Greenville Rivet Joint
GTRI
Charleston (2): SSC Data Ctr, MEF-MEU
Ft Huachuca: (5) JITC, JTDL, CMIS, JTRS, EPG
Ft Hood (2): CTSF, TTEC
Eglin AFB (5): AOC, DTF, GWEF, KHILS, JDAT
LMCO Global Vision Network
Melbourne NGC JSTARS

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 (2): SCSC, SSDS
Newport News NGC VASCIC
McLean MITRE NSEL
Metro Park JMETC / TENA SDA Lab
Richmond NRO CTE

Army
Air Force
Navy
Marines
Joint
Industry

As of 12 Nov 2015

DISTRIBUTION A. Approved for public release: distribution unlimited.

How a Customer Views JMETC

Availability of Geographically Separated T&E Assets

All linked by JMETC

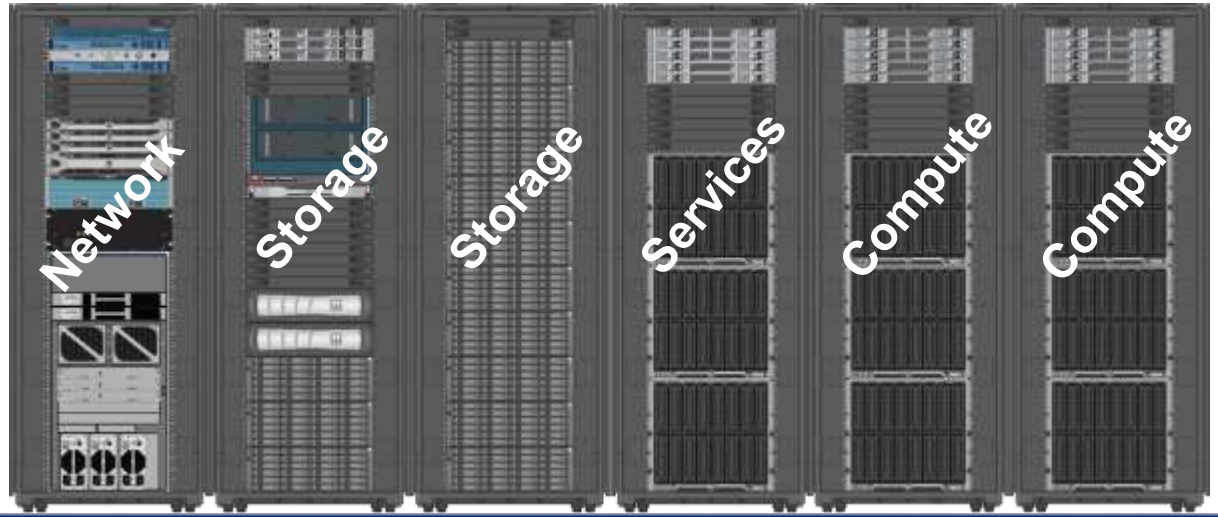
Major FY15/16 Events

JMETC Secret Network (JSN)

Customer	Event	Execution Dates	Onsite Support
Joint	Joint Interoperability Test Command (JITC) Joint Interoperability Tests (JIT)	(Four Events/FY) Last Event: Feb 1 – 26, 2016 Next Event: April 4-15, 2016	**Yes**
Navy	MQ-4C Triton	Mar 1, 2015 – Mar 1, 2016	**-**
Air Force	Small Diameter Bombs II (SDB) Live Fly Testing	Last Event: August 24 – 28, 2015 Next Event: (AGILE) Aug/Sep 2016	**-**
Navy	Aegis Ballistic Missile Defense (BMD) 4.0.3 Testing	(Three Events in FY15) Last Event: Feb 24 - 27, 2015 Next Event: TBD	**Yes**
Navy	Interoperability Development and Certification Testing (IDCT) Distributed Integration & Interoperability Assessment Capability (DIIAC) and Multi Site Training (MST)	(Four Events/ FY) Last Event: Nov 02-06, 2015 Next Event: Mar 7 - 18, 2016	**Multiple**
Joint	Joint Unmanned Air System – Mission Environment (JUAS-ME)	(Three Events/FY) Last Event: Sep 15-17, 2015 Next Event: TBD	**Yes**
Air Force	Air Force Systems Interoperability Test (AFSIT)	(Four/Five Events/FY) Last Event: Feb 1 - 26, 2015 Next Event: June/July 2015	**-**
Joint	F-35 Joint Strike Fighter Record & Playback	(Three Events/FY) Last Event: Aug 24-28, 2015 Next Event: Aug 2016	**Yes**
Joint	DIIAC Ballistic Missile Defense (BMD) Fleet Synthetic Training (FST) Testing	Jun 8-12, 2015	**Yes**
Navy	Aegis Integrated Air & Missile Defense (IAMD) Baseline 9C1D Training Test	30 Mar - 3 April, 2015	**-**
Air Force	Tinker Block 40 / 45 Testing	30 Mar - 3 Apr, 2015	**-**
Coalition	Joint Integrated Air & Missile Defense Office Correlation / Decorrelation Interoperability Test (C/DIT)	Oct 21-23, 2015 Next Event: Sep 19 - 23, 2016	**Yes**
Air Force	Simulation Exercise (SIMEX)	Dec 14 – 18, 2015	**Yes**

Regional Service Delivery Points (RSDPs)

- Hosted on the JMETC MILS Network (JMN)
- 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

JMETC MILS Network (JMN)

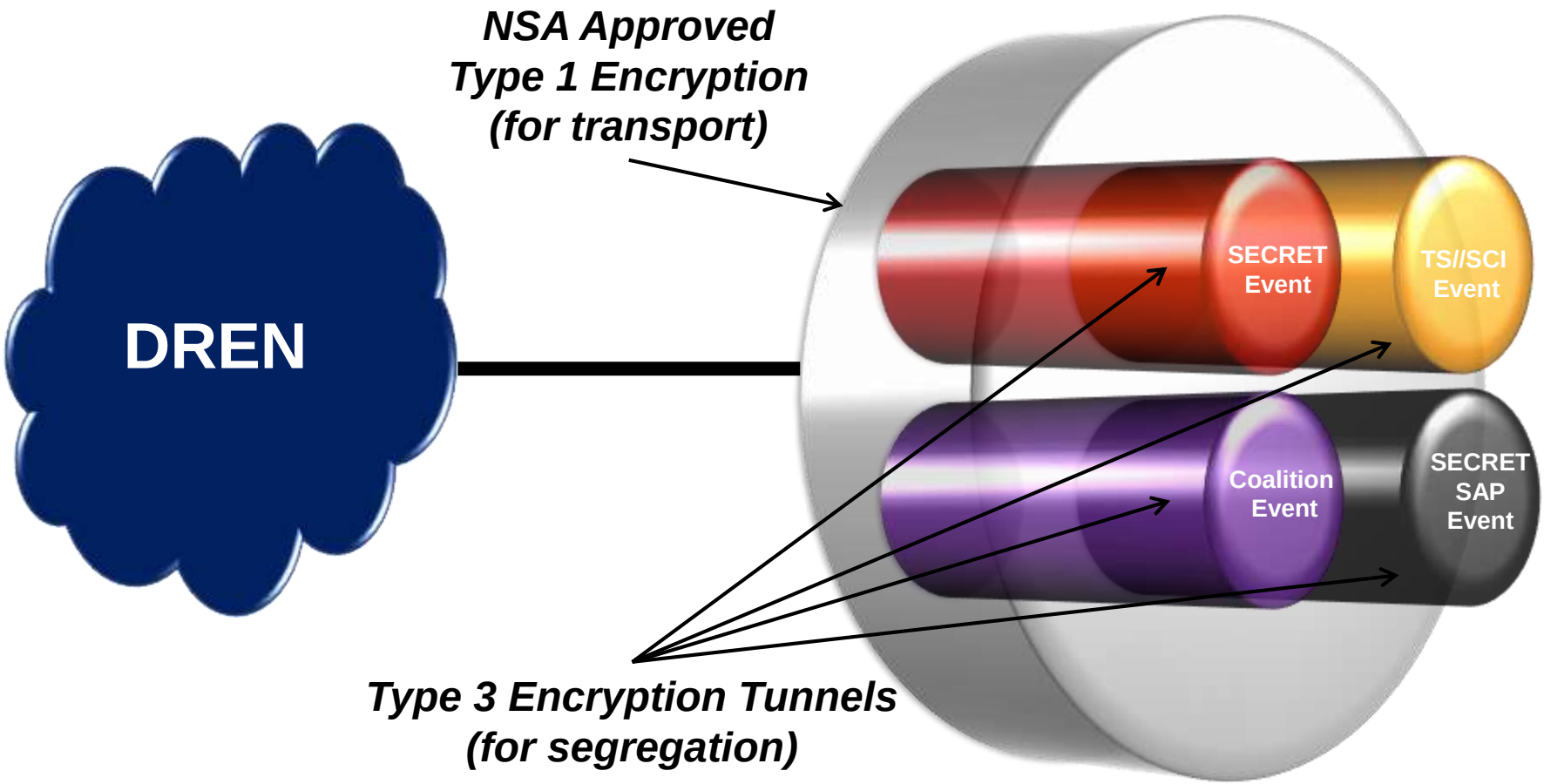
- Objective is to provide 1) access to ***enterprise resources, tools and services*** at ***higher classifications*** and 2) ***isolated distributed testbeds*** ***on a CLOSED network*** to meet growing interoperability and Cyber T&E requirements
  - Accredited by DIA to operate up to TS//SCI/SAP/SAR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



RSDP CONOPS

- Accessibility by users
  - Sites/users can utilize any RSDP (assuming latency is not an issue)
  - Sites/users can conduct multiple events, at multiple classifications on multiple RSDPs concurrently
- Extensibility to address extremely large scale, high fidelity requirements
  - Multiple RSDPs can be used in conjunction to support a single event
  - A RSDP can be used in conjunction with other Cyber capabilities (e.g., NCR) as part of a larger virtual environment
- Technical support personnel available to users/events
  - Event Leads to help refine requirements and plan/design events
  - RSDP Engineers then create the representative cyber environment on the RSDPs
- Resource prioritization by JMETC Program Office
- Remotely managed by the JMETC NOSC

RSDP: Status

- **Resources accessible via the JMN**
- **Deployment Schedule**
  - Development RDDP #0 and RSDP #1 are operational
  - RSDP #2 Operational
  - RSDP #3 has been installed with anticipated availability this month
  - RSDP #4 & #5 are awaiting facility upgrades scheduled to be completed by end of this year
  - Additional RSDPs planned for FY17
- Events
  - Already supported
    - Cyber infrastructure and tool evaluations
    - Regression testing
    - Scalability assessments
    - CMF Training
    - Capability assessments
  - Late stages of planning
    - Risk reduction for IA patch deployment to afloat systems

JMETC Challenges

Command Post of the Future (CPoF)

- Army Program
  - Needed to test software scalability
  - Working up to 5000 extremely high fidelity nodes
  - Timing was critical
- Crawl, Walk Run
  - Started at 100 nodes
  - Progressed to 500 nodes
  - Final test at 5000 nodes for 60 days constant testing
- Accommodations Made
  - Significant JMETC engineering time
  - Purchased high IO rate storage devises
  - Provided an entire RSDP (the only one at that time) for 60 days
    - Ran 60 days, 24 hours per day
- CPoF got the data it needed!

Cybersecurity Test Requirements Challenge

- A program says, “I need to do cybersecurity testing. What do I need to do?”
- Answer, execute a Cybersecurity Table Top
  - Two Opposing Teams and a Control Team - Mission Forces (Blue), Opposing Forces (Red) and controllers (White)
  - White gives Blue and Red their missions
  - Each goes of to plan their mission
  - Blue and Red then come together to discuss how they each would conduct their missions
    - What works and what does not work
    - Blue wants to remain Fully Mission Capable (FMC); Red wants to make Blue Not Mission Capable (NMC); May need to iterate
  - Conduct analysis and Bin vulnerabilities discovered
    - Low risk; no further action
    - High risk; need to fix and test the fix
    - Questionable; need further examination and test

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

Army Cyber Training Requirements Challenge

- Training Army Cyber Mission Forces
  - Multiple students training simultaneously
  - Training at different levels of proficiency
  - Training access 24/7
- Solution
  - Worked with Army Cyber Center of Excellence (CCoE)
  - Developed “virtual class rooms” for levels of training
  - 42 class rooms currently available; multiple classrooms for each level
  - Working with CCoE trainers and engineers to develop added class rooms – up to 85 in the next few months

Other Challenges

- People Challenges
  - Finding personnel with the required mix of skill sets
  - Retaining those people
  - Addressing through internal training, TRMC STEM Initiative, and automation
- Automation to reduce numbers of people required
- Technical Challenges
  - Line speed, Type 1 encryption for data at rest
    - Would permit storage of multiple classifications on one storage device
    - Assessing three possible solutions

Summary

- JMETC infrastructure has been enhanced to support Interoperability and Cyber Security testing
- JMETC is increasing capabilities to support the ever growing demand signal for Cyber Security testing, training, and experimentation
- Enables Acquisition and T&E to partner for:
  - Better product
  - Reduced time
  - Lower cost

JMETC Program Points of Contact

JMETC Program Manager:	**Chip Ferguson** benard.b.ferguson.civ@mail.mil 571-372-2697
JMETC Lead Operations Planning:	**Marty Arnwine** martemas.arnwine.civ@mail.mil 571-372-2701
JMETC Lead Engineering:	**AJ Pathmanathan** arjuna.pathmanathan.civ@mail.mil 571-372-2702

www.jmetc.org

Questions?