30TH ANNUAL INTERNATIONAL

Test and Evaluation

SYMPOSIUM

JOINT MISSION ENVIRONMENT TEST CAPABILITY (JMETC)

Cyber T&E Initiatives

AJ Pathmanathan

JMETC Deputy PM for Engineering

NCR Technical Director

November 14, 2013

GET CONNECTED to LEARN, SHARE, and ADVANCE

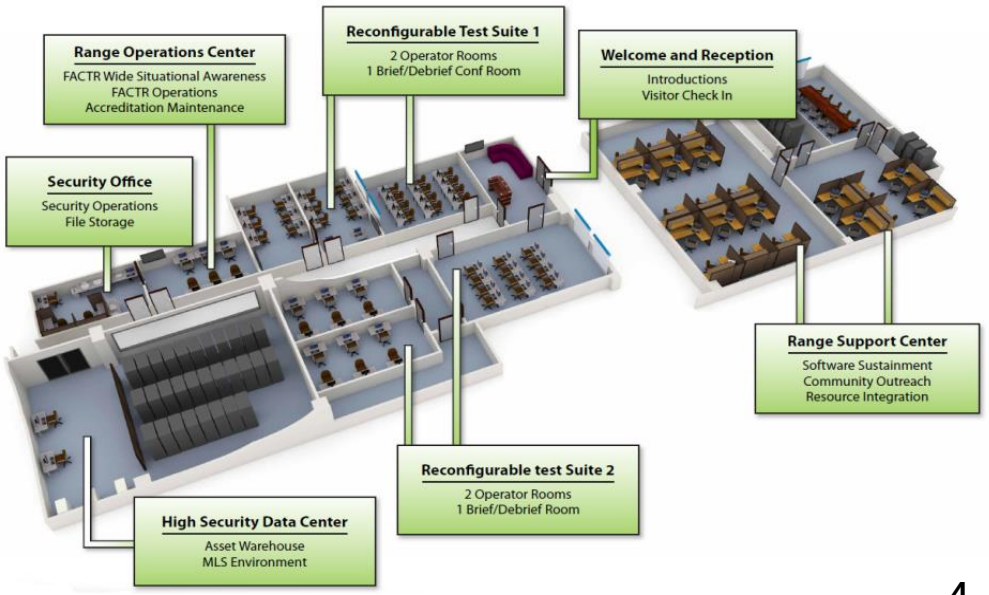
DISCUSSION TOPICS

- Enhanced Distributed Test Infrastructure
- National Cyber Range (NCR)
- Regional Service Delivery Points (RSDP)
- Additional Cyber T&E Initiatives

National Cyber Range (NCR)

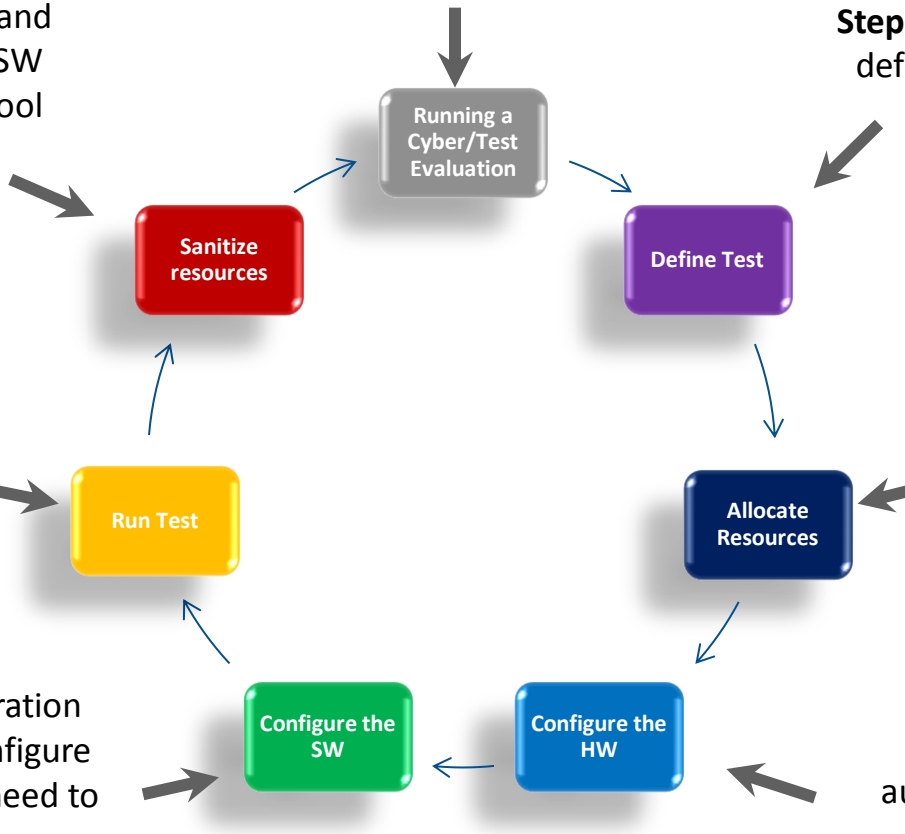
NATIONAL CYBER RANGE (NCR) ORLANDO, FL

- **Oversight**
  - Transitioned program from the Defense Advanced Research Projects Agency (DARPA) to the TRMC in October ’12
  - TRMC charged with functionalizing the capabilities for use by the Test, Training, and Experimentation communities
- **Goal**
  - Create a secure, self-contained facility that can rapidly emulate the complexity of defense & commercial networks, allowing for cost-effective and timely testing
- **Range Features**
  - Automated range build-out capability
  - Automated range sanitization
  - User friendly environment design and test planning tools
  - Supports multiple concurrent tests events at varying classifications



NCR AUTOMATED CYBER TEST PROCESS

Start with a common pool of HW /SW Resources and Cyber Tool Set



Step 1: Utilize Test Spec Tool to define end to end aspects of test

Step 2: Automated Scheduler determines what resources from the pool are needed and allocates them to test

Step 3: Range Configuration Tools automatically wire HW to the appropriate configuration

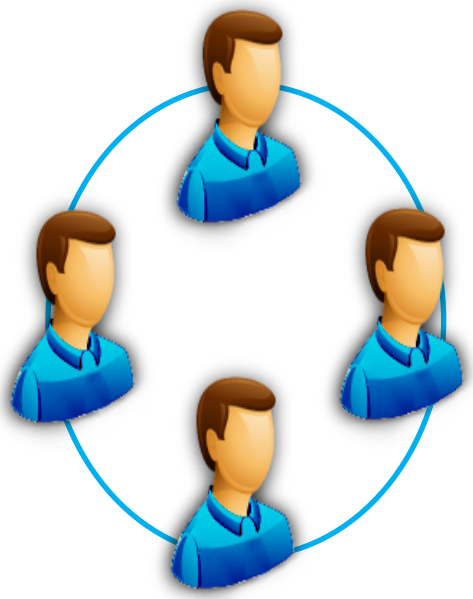
Step 4: Range Configuration Tools automatically configure and verify the SW you need to run test

Step 5: Test team validates environment, installs System Under Test and runs test/collects data using toolset

Step 6: Sanitize HW and "virtually" put HW/SW resources back in pool

Efficiency and Accuracy via Automation

NCR TEST TEAM



- Flexible Model
  - End to end test support
  - You give us a test specification or asset list and we give you a configured or empty testbed
- Other services
  - Cyber and testing SME
  - Develop threat vectors
  - Custom traffic generation
  - Custom sensors and visualization
  - Integrate custom devices or software assets
  - Custom data analysis
- Easily incorporate distributed event resources
  - Remote red/blue teams
  - Specialty or kinetic assets
  - Additional computing resources

NCR Event Examples

- **HONOR**: US Pacific Command (PACOM) sponsored event to test scalability of the Virtual Secure Enclave (VSE) Architecture
  - **25 trials executed over 108 hours (8 AM Monday to 8 PM Friday)**
    - **Automated Reconfiguration & Data Collection: 45 hours**
    - **Test Time: 63 hours of testing time**
    - **Testing Intervals: 1.8 hours**
    - **Efficiency: 58.3%**

- **JAVELIN**: DOT&E sponsored event to demonstrate interoperability with other DoD cyber testing resources (JCOR, Sandia, TSMO)
  - **JCOR/NCR Shared Infrastructure**
    - **Network infrastructure**
      - **Control network: DHCP hosted at NCR**
      - **Experiment network: DHCP hosted at JCOR**
    - **Control infrastructure**
      - **Experiment coordinated from NCR**
      - **Log collection and environment reset centrally executed from NCR**
    - **Host configuration**
      - **Single NCR-provided VM image was used at both NCR and JCOR**
  - **Conducted at different classifications concurrently**

Enables large-scale scenarios to be tested efficiently

Regional Service Delivery Points (RSDPs)

REGIONAL SERVICE DELIVERY POINTS (RSDPS)

- **The Regional SDPs (RSDPs) will:**
  - provide increased *capacity and scalability* to create persistent, representative cyber-threat environments
  - provide *common range services* (i.e. traffic generation, simulation, instrumentation, visualization, and integrated event management)
  - be *flexible and adaptable* to evolving users requirements
  - leverage the latest technology to deliver *cost and performance efficiencies* (virtualization, rapid reconstitution)
- **Challenge: Accreditation of MILS architecture**
  - Potential hurdles with sanitization and segregation

Address Capacity & Capability Gaps

RSDP: SCHEDULE

- **Successful RSDP Capability Demonstration conducted May 30st at TSMO**
  - **Linked prototype RSDP and 1st production RSDP**
  - **Established a baseline metric of platform performance**
  - **Established resource baseline to manage and operate**
  - **Demonstrated ability to share resources**
  - **Demonstrated integration of traffic generation capability (MIT Lincoln Labs LARIAT 8.6 and 9.0)**
  - **Demonstrated ability to deploy virtual environments**
    - **Constructed a Terminal Fury size event environment in ~5 hours (previously took ~6 weeks)**

- **Deployment**
  - **Prototype to stay at TSMO for continued development**
  - **Production RSDPs to be geographically dispersed**
    - **1st production RSDP homed to TSMO**
    - **2nd production RSDP placement TBD (Nov 2013)**
  - **Expect 1 RSDP per year over the FYDP**

OTHER CYBER INITIATIVES

CYBER RANGE INTEROPERABILITY STANDARDS (CRIS)

- TRMC sponsored WG supported by MIT Lincoln Laboratories
  - Government, Industry and Academia
- Cyber Ranges have been independently developed
  - Tools
  - Processes
  - Architectures
  - Underlying Technologies
  - Lexicon
- Result is stovepipe solutions that are difficult to integrate
  - Limited scalability
  - Increased cost and schedule
- Goal: Identify key interoperability gaps and recommend solutions/approaches
- Task Status
  - Lexicon: incorporating feedback for release in December
  - Range Process: incorporating feedback with anticipated release in December
- Next Steps:
  - Pilot Project to address Environment Generation

Enable Interoperability through Standardization

ADDITIONAL TRMC INVESTMENTS

- **T&E/S&T Cyber Test Technology (CTT) Sponsored Efforts**
  - Expand upon current automated sanitization capabilities for Cyber environments
  - Develop models for accurate, large scale cyber threat simulation at all layers of the OSI model
  - Develop automated threat portrayal capability
  - Status
    - Award made to Georgia Tech Research Institute in March 2013 to develop "Red Team-in-a-Box" with anticipated completion in FY16
    - Award made to Lockheed Martin in June 2013 to develop enterprise sanitization capability with anticipated completion in FY16
    - Anticipate successful completion of award made to Scalable Network Technologies for development of high fidelity, large scale network emulation in FY14

- **Central T&E Investment Program (CTEIP) Sponsored Efforts**
  - Develop enhanced defensive Cyber instrumentation
  - Develop enhanced LVC representations of large scale operational environments
  - Status
    - In early development with SPAWAR to develop Cyber T&E specific instrumentation and high fidelity, large scale, operational representative environments with anticipated completion in FY17-18

- **JMETC FY14 Tool Focus Areas**
  - Cyber T&E planning, execution and analysis tools
    - Environment Generation
    - Visualization
    - Non-intrusive Instrumentation
    - Real-time analysis
    - Automation
    - More…

Enhanced
Distributed Test Infrastructure

ENHANCED DISTRIBUTED TEST INFRASTRUCTURE: OVERVIEW

- **Maintain all current JMETC key tenants**
  - Access to Industry and Academia (e.g., Boeing LabNet)
  - Access to other DoD networks (e.g., JTEN)
  - Help Desk
  - Persistent Connectivity (e.g., standing IA agreements, continuous network performance characterization, proactive troubleshooting)
  - Enterprise Services (e.g., VoIP, CHAT, Adobe Connect, patch servers, DNS, file transfers, NTP, Anti-Virus Updates, etc.)
  - Onsite Event, Network and IA Support
  - Distributed Test Tools
- **Proposed Enhancements**
  - Support classifications up to TS/SCI
  - Enterprise Coalition connectivity solution
  - Incorporate RSDP capability (i.e., cloud based services such as tools, instrumentation, traffic generation, and virtual environments)
  - RDT&E DAA

Support both Interoperability and Cyber T&E requirements

DISTRIBUTED TEST INFRASTRUCTURE ENHANCEMENTS: CHALLENGES, SCHEDULE & COST

- Challenges: we are breaking new ground
  - Not a fully closed environment… access to other networks
  - Certification by Defense Intelligence Agency (DIA)
  - Acceptance by the SAP community
- Transition Schedule
  - IOC expected in late 1Q FY14
    - Initial sites driven by DOT&E cyber requirements
  - FOC expected 12-24 months later
    - Transition all existing sites (currently 75 with 16 planned)
    - Establish "peering" back to legacy infrastructure to maintain connectivity during transition
- Cost: JMETC intends to cover all transition costs for existing sites
  - Non-Recurring Costs (e.g., hardware, installation, etc.)
  - Annual Recurring Costs (e.g., operations, maintenance, IA, etc.)