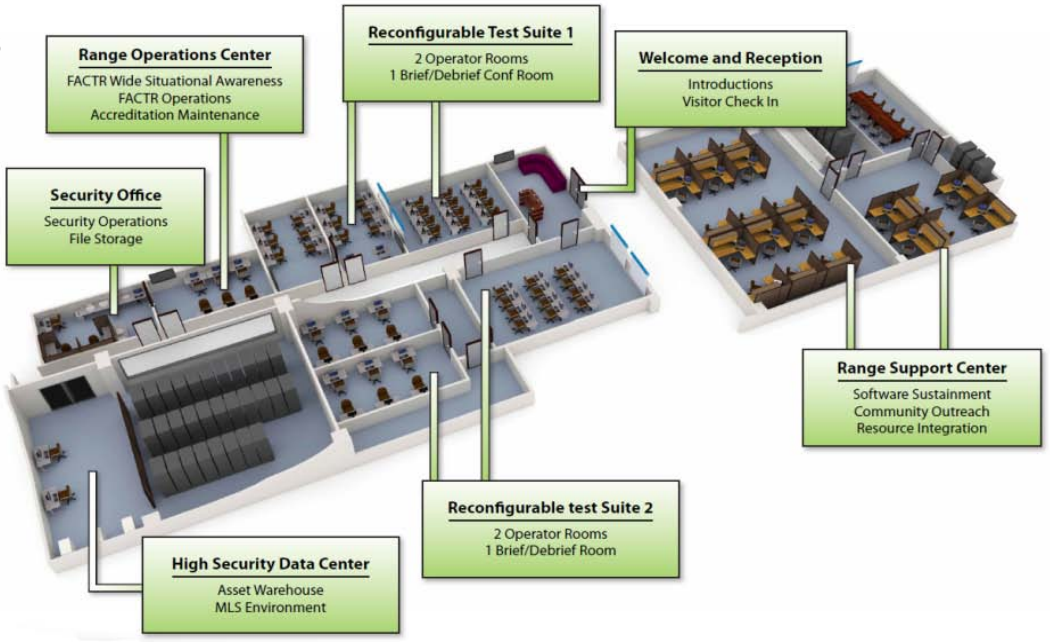
Test Resources Management Center (TRMC)

Cyber T&E
Infrastructure Resources and Initiatives

AJ Pathmanathan
JMETC Deputy PM, Engineering
January 29th, 2015

National Cyber Range (NCR)

- Provides a state of the art capability to very rapidly to generate representative cyber environment testbeds
  - Comprised of computational and storage assets to host ~ 50K high fidelity virtual representations
  - Capable of supporting 4 testbeds at varying classifications concurrently
- Designed with a focus on the automation tool suite to minimize environment design, generation, recreation, and teardown timelines
  - User friendly environment design and test planning tools
  - Automated range build-out capability
  - Automated execution with scripted runs
  - Automated range sanitization
- Facility is capable of supporting multiple events onsite
- SME support for planning, designing and execution of events



NCR Status

- Transitioned from DARPA and functionalized FY12
- NCR supports a wide variety of cyber event types
  - R&D
  - DT&E
  - Product evaluation
  - Training events
  - Mission rehearsal
  - Compliance testing
  - Risk reduction activities
  - Architecture analysis
  - OT&E
  - Malware analysis
  - Forensic analysis/Event Reconstruction
- Utilization
  - 96% FY 14 (scheduled)
  - 76% in FY 15 (currently scheduled)
- Level of support from NCR is dependent on customer needs

NCR Event Example

- PM is “Shifting Left”
  - Using DT&E for risk reduction/rehearsal for OT&E

- PO and Prime teamed with NCR and the Navy Red Team
  - Together developed and designed the test plans and scenarios
  - NCR team generated the virtual environment
  - Executed using real operational plans and validated threats
  - NCR team collected and assisted in the analysis of the resulting data

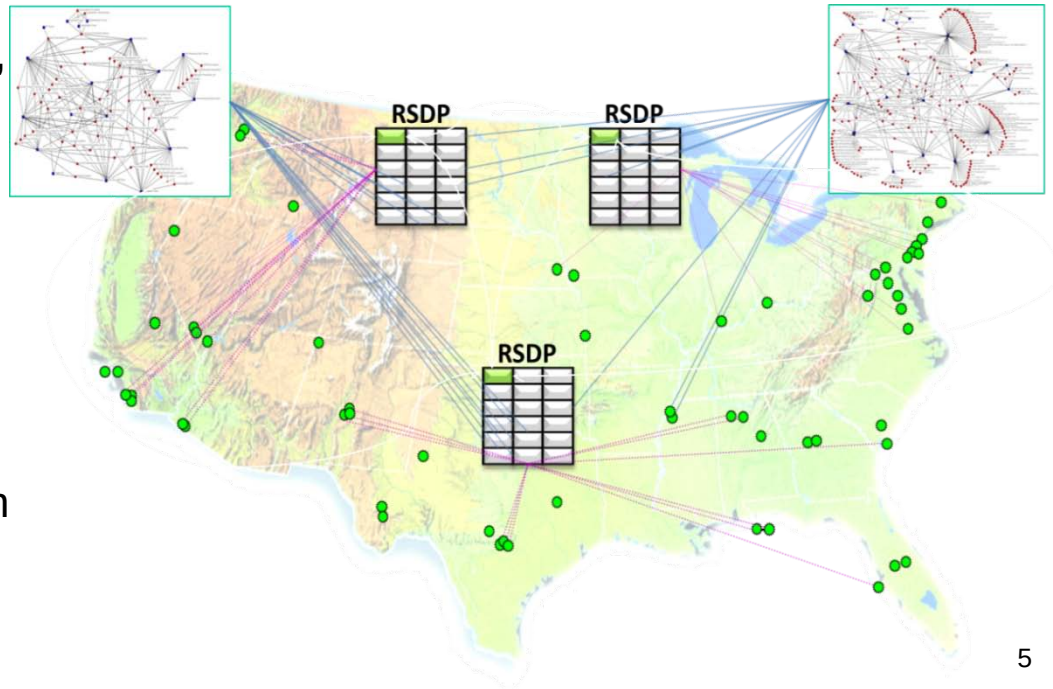
- Benefit to the PM
  - Provided empirical data to help understand the cybersecurity trade space
  - Led to refinements of the program’s overall Cyber T&E methodologies and approach

- PM intends to conduct additional cyber T&E events on the NCR as system matures

Regional Service Delivery Points (RSDPs)

- Provide more generalized enterprise resources to generate virtualized representative cyber environments
  - Comprised of computational and storage assets to host ~15K high fidelity virtual representations
  - 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)

- Designed to be adaptable, flexible, and cost-effective
  - 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



RSDP Status

- Deployment Schedule
  - Development testbed and RSDP #1 are operational
  - RSDP #2 currently being installed with anticipated availability in March/April 2015
  - RSDP #3 is prepped for shipment and install
  - Additional RSDPs planned for FY15 and FY16

- Events
  - Already supported
    - Cyber infrastructure and tool evaluations
    - Regression testing
    - Scalability assessments
    - Capability assessments
  - Late stages of planning
    - Risk reduction for IA patch deployment to afloat systems
    - Large scale training events
    - Capability assessments
  - Several others in early planning stages

Enhanced Distributed Testing Infrastructure

- Requirement Driver: limitations with our **JMETC SECRET Network (JSN)** infrastructure to support Cyber T&E
  - Cannot fully leverage existing and emerging cyber capabilities (e.g., NCR, RSDPs, etc.)
  - Limited to SECRET Collateral
  - Lack of secure “sandbox” for release of malicious code w/ minimized risk of propagation

- Solution: The **JMETC MILS Network (JMN)** serves as the RDT&E enterprise network solution for Cyber T&E and all higher classifications requirements
  - JMN employs the Multiple Independent Levels Security (MILS) Architecture
    - Allows for logical segregation of data classifications, environments, and users
    - Affords site ability to support multiple classifications concurrently via one network stack
  - Accredited by the Defense Intelligence Agency (DIA)
  - Operates over DREN and managed by the JMETC Network Operations Security Center (NOSC)
  - Will continue to leverage the JSN (which operates on SDREN) to serve as the RDT&E enterprise network solution for distributed testing requirements at the SECRET classification

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**
- Upcoming Deliverables
  - Lexicon
  - Cyber Range Process
  - Prioritized Interoperability Gaps

Enable Interoperability through Standardization

Additional TRMC Cyber Investments

- T&E/S&T Cyber Test Technology (CTT) Sponsored Efforts
  - Award made to Georgia Tech Research Institute develop automated threat portrayal capability
  - Award made to Lockheed Martin to develop enterprise sanitization capability
- Central T&E Investment Program (CTEIP) Sponsored Efforts
  - SPAWAR funded to develop Cyber T&E specific instrumentation and high fidelity, large scale, operational representative environments
- JMETC Tool Investments Focus Areas: planning, execution and analysis
  - Environment Generation
  - Visualization
  - Non-intrusive Instrumentation
  - Real-time analysis
  - Automation

Questions?

AJ Pathmanathan
JMETC Deputy PM, Engineering
arjuna.pathmanathan.civ@mail.mil
571.372.2702