Joint Mission Environment Test Capability (JMETC)

Enabling Distributed Cybersecurity T&E

AJ Pathmanathan
JMETC Deputy PM for Engineering
08 October 2014

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 environments

JMETC Connectivity

Functional Sites: 77
New Sites Planned: 11
Connection Points to Other Networks: 7

- SECRET Defense Research & Engineering Network (SDREN) for network connectivity
- Encrypted for Secret – System High
- Pro-active monitoring of network for optimal performance
- Capable of supporting numerous simultaneous test events

Boeing LabNet Tukwila
Keyport NUWC

Site in Alaska
Ft. Greely: CRTC

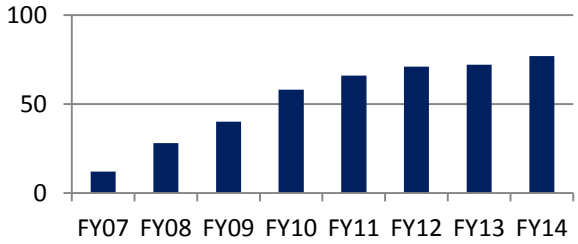
Edwards (2): Ridley
412th EWG IFAST
China Lake (3): F/A-18, IBAR, TSPIL
Point Mugu (3): ITEC, EA-6B. EW CyCon
Camp Pendleton: MCTSSA
Corona: NSWC
Palmdale, Triton
Point Loma :
SSC-PAC 59140
SSC-PAC HAIPE
SSC-PAC JEDI
West Agg Rtr.
Rancho Bernardo, NGC Triton

Sites in Hawaii
PMRF: Bldg 105
MHPCC

Dugway Proving Ground
Raytheon Tucson
Yuma PG
Kirtland AFB DMOC
Tinker AFB AWACS
Ft. Sill (2): FSED, SMART Lab
WSMR IRCC
Ft. Bliss MCC
Ft Huachuca: (5) JITC, JTDL, CMIS, JTRS, EPG
Ft Hood (2): CTSF, TTEC
Greenville Rivet Joint
Boeing LabNet Berkeley
Crane (2): NSWC RDT&E, NTN Lab
WPAFB: SIMAF
Redstone (10): SMDC RTC: DTCC, DISTL SED: Patriot, THAAD, FAAD, GSIL, JLENS, MUSE, C-RAM
AMRDEC
GTRI
Charleston (2): SSC Data Ctr
MEF-MEU
WNW
Eglin AFB (5): AOC, DTF, GWEF, KHILS, JDAT
CCF
LMCO Global Vision Network
Melbourne NGC JSTARS

Rome NY AFRL
Hanscom AFB CEIF
Newport NUWC
Bethpage: NGC Triton
Bethpage: NGC Triton
Moorestown: CSEDS

Aberdeen:
ATC-STE
SRW RIL
Pax River:
(9) E2C, E2D, MCL, ACETEF, SAIL, ATR, E-2C SIL, UASIL, MFS
JMETC SYSCON
East Agg Rtr.
Dahlgren:
(2) CEDL,IWSL
(1) Rapid-SIL/C2
JS J8 DDC4 C4AD
Langley TDLITC
Norfolk COMOPTEVFOR
Dam Neck CDSA
Wallops Island (2): SCSC, SSDS
Newport News NGC VASCIC
McLean MITRE NSEL
Kingstowne JMETC / TENA SDA Lab

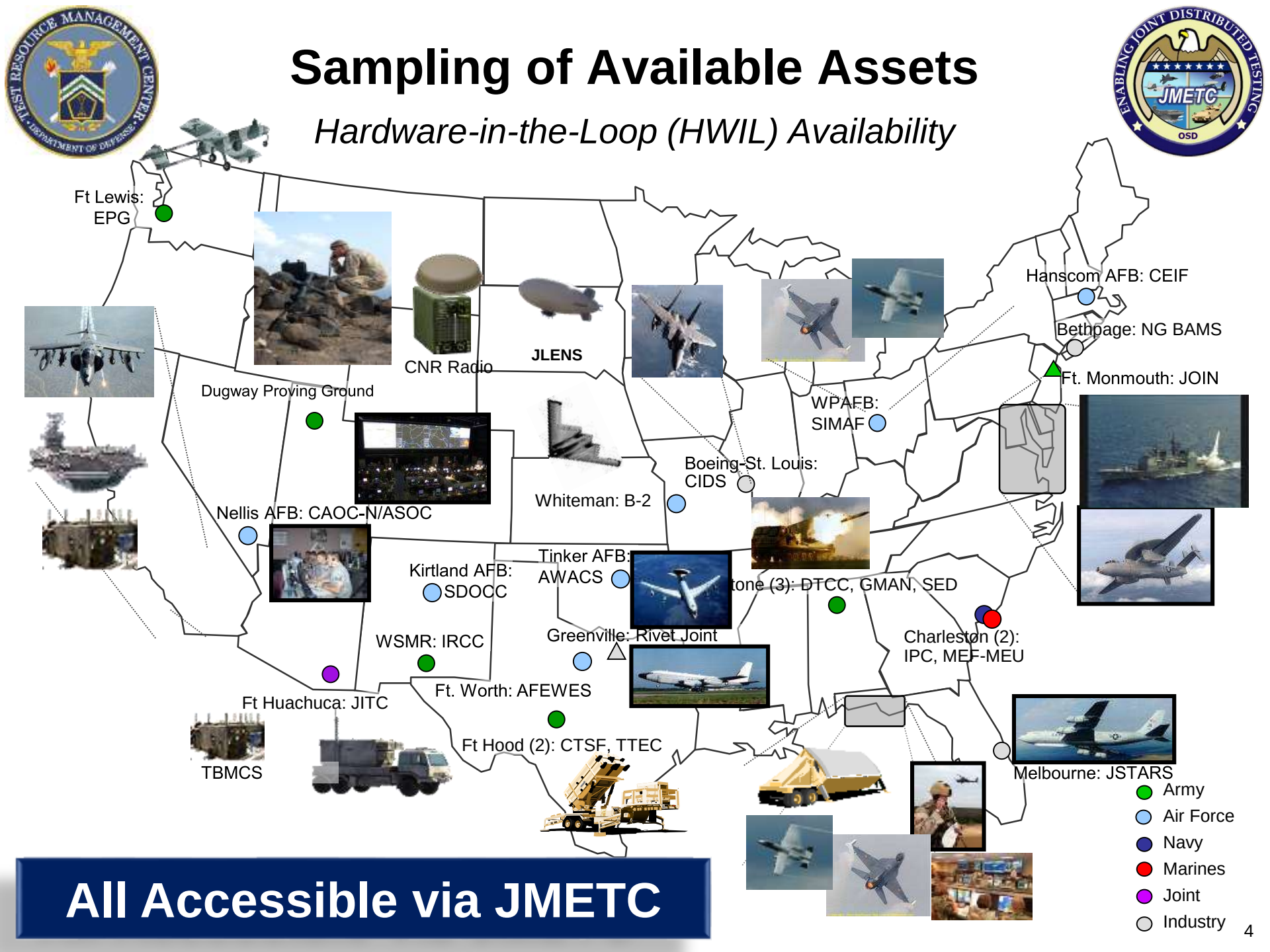


As of September 2014

Army
Air Force
Navy
Marines
Joint
Industry
Academia

Sampling of Available Assets

Hardware-in-the-Loop (HWIL) Availability



All Accessible via JMETC

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**

Current Distributed Test Network Gaps

- Current Solution: Use SECRET Defense Research & Engineering Network (SDREN)

- Current Limitations
  - Cannot support SECRET SAP/SAR, TS, TS//SCI, TS//SCI/SAP/SAR (currently limited to SECRET)
  - Inability to bridge kinetic and non-kinetic assets and environments
  - No access to National Cyber Range (NCR), Regional Service Delivery Points (RSDPs), and other Cyber T&E resources
  - Extremely limited access to partner nations
  - Inability to support Tactical IP addressing schema

“JMETC 2.0” Testbed: Pilot Events

- Accredited by Defense Intelligence Agency (DIA)
  - Approved to operate up to TS//SCI
- Several pilot events executed to assess and refine proposed approaches
  - Assess processes, procedures, and CONOPS (e.g., event request, environment creation, distributed NOSC coordination, event documentation, personnel requirements, etc.)
  - Assess network performance/optimization
  - Streamline and document processes and procedures
  - Define internal and external roles & responsibilities
  - Collect lessons learned
  - Establish procedure to “peer” to Joint Information Operations Range (JIOR)
    - “no cost” access to Training and Experimentation Communities’ sites & capabilities
- Finalized enhanced architecture agreed to early September 2014

JMETC Enhanced Distributed Test Infrastructure CONOPS

- Unified Network Infrastructure Approach: continued partnership with HPCMO using DREN as underlying service provider
  - Core Network (SDREN)
    - Network connectivity managed by SDREN NOC and accredited by HPCMO DAA
    - Persistent connections (network is optimized and always available for use)
    - Single level of security: SECRET
    - End-to-end technical support (online helpdesk, phone and onsite) and services provided by JMETC
  - Enhanced Network
    - Established based on lessons learned from JMETC 2.0 pilot events
    - Connectivity managed by JMETC Network Operations Security Center (NOSC) and accredited by DIA
    - Event specific Virtual Private Networks (VPNs) created for limited duration
    - Multiple Independent Levels of Security (MILS) Architecture
      - Support data classifications up to and including TS//SCI/SAP/SAR
      - Support Coalition connectivity
    - Support embedded Tactical IP addressing schema (including non-routable IP addresses)
    - Technical support provided by JMETC Technical Team when “read on” to the program

Next Steps

- Finalize Accreditations
  - Incorporate new name
  - Attain SAP Approval from DoD SAPCO
- Finalize Funding Model
  - Intent is that all costs for the Enhanced Infrastructure (both non-recurring and annual recurring) are institutionally funded by JMETC
  - Dependent on available resources
- Socialization within the Community
  - Revive JMETC User Groups (tentative)
  - Telecon/Direct-Connect Online (DCO) sessions
  - Website (e.g., FAQs, factsheets, feedback reflectors, etc.)
  - Community Forums
- Implementation
  - Four (4) pilot sites (Dahlgren, Dam Neck, Patuxent River, & TSMO) currently online
  - New sites prioritization based on test schedule
  - Near-term deployment limited by availability of Service Delivery Points (SDPs)

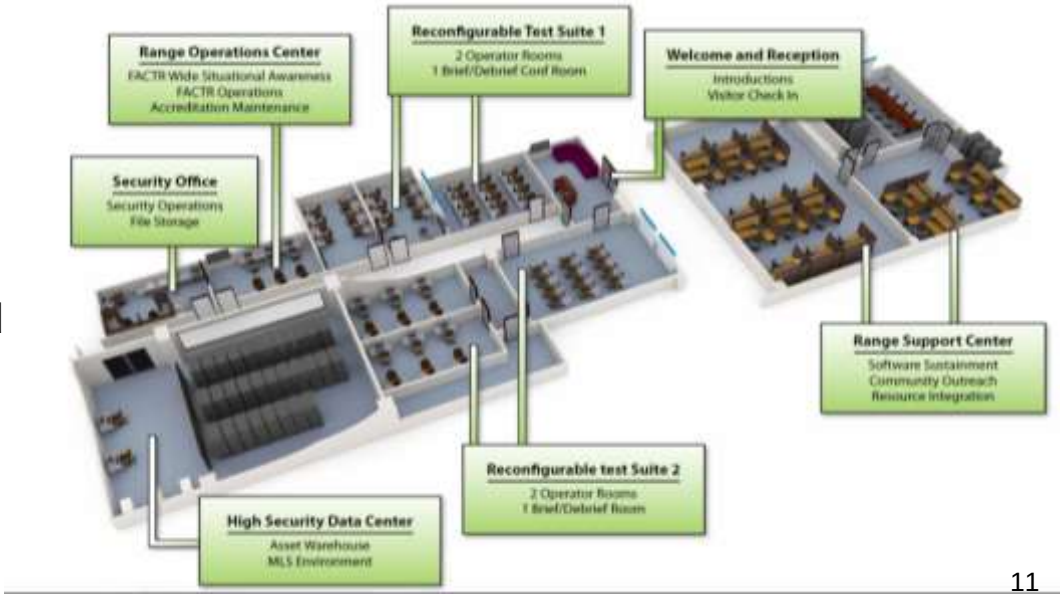
National Cyber Range (NCR)

National Cyber Range (NCR) Orlando, FL

- **Oversight:**
  - Transitioned program from the Defense Advanced Research Projects Agency (DARPA) to the TRMC in October 2012
  - TRMC charged with “functionalizing” the capabilities for use by the Test, Training, and Experimentation communities

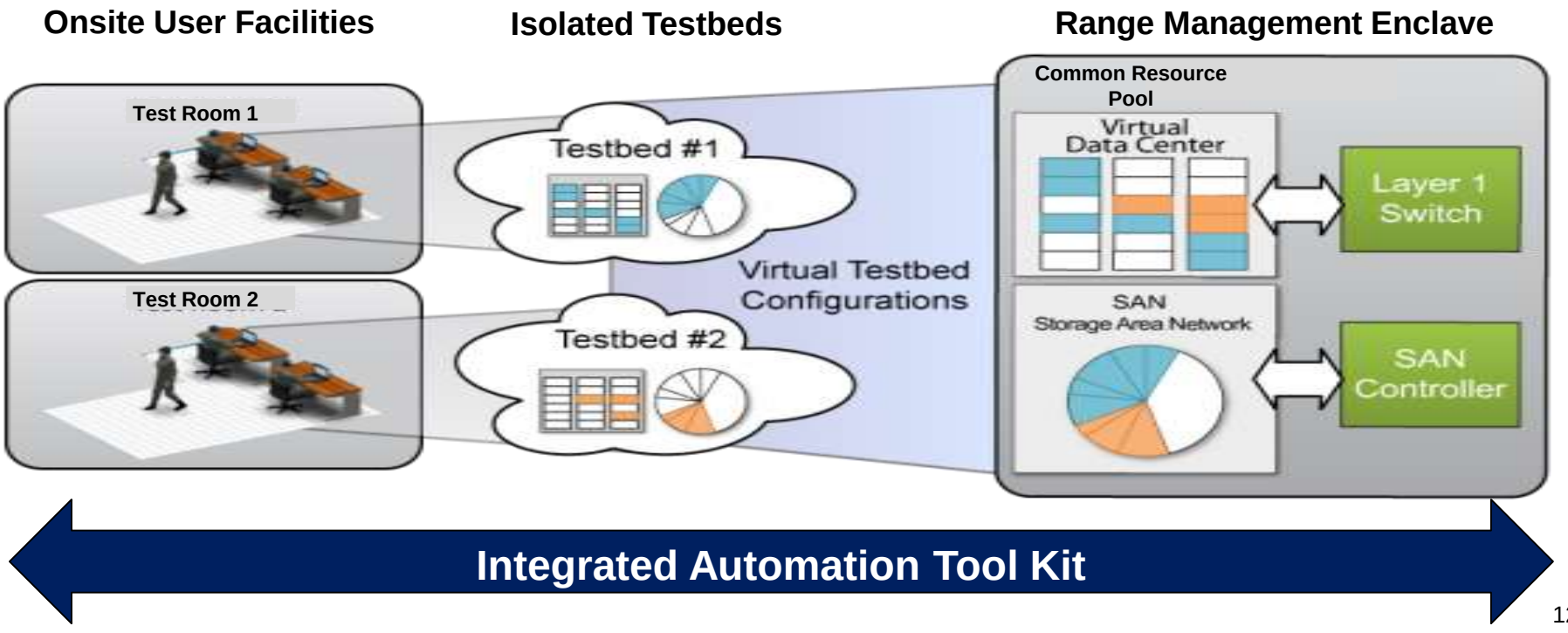
- **Goal**
  - Create a secure, controlled facility that can rapidly emulate the complexity of defense & commercial networks, allowing for cost-effective and timely testing in support of the full spectrum of Cyber activities

- **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



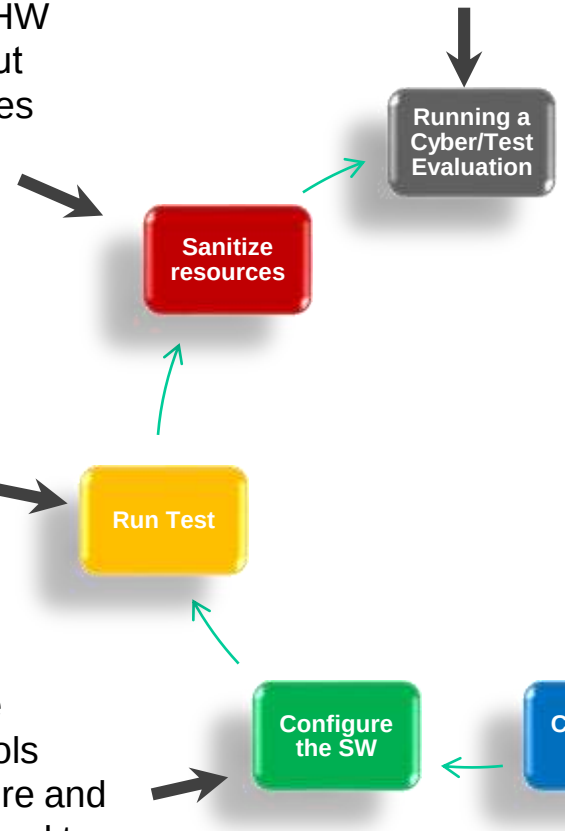
NCR Concept Overview

- Common pool of computing and storage resources that can be:
  - Partitioned into multiple testbeds capable of operating at varying classifications concurrently
  - Provide controlled environments in which malicious code can be released
  - Rapidly configured to provide large scale, operational representative networks
  - Provide ability to sanitize exposed systems so they may be reused



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

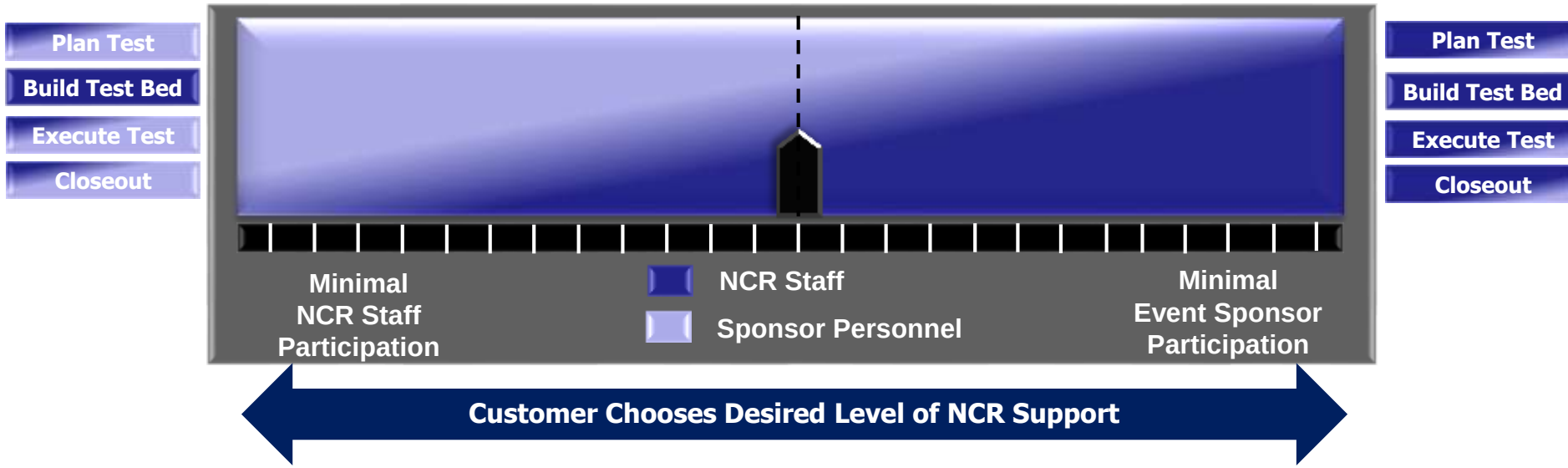
Support Spectrum

Extreme Use Case: Minimal NCR Support

- NCR Staff delivers verified test bed environment and port test sanitization
- Event Sponsor personnel do everything else

Extreme Use Case: Maximum NCR Support

- NCR Staff works w/ event sponsor to define the environment and tests
- NCR Staff essentially does everything else with periodic review



- Easily incorporate distributed event resources
  - Remote red/blue teams
  - Specialty or kinetic assets
  - Additional computing resources
- Other services
  - Develop threat vectors
  - Custom traffic generation
  - Custom sensors and visualization
  - Custom data analysis

Supported Event Types

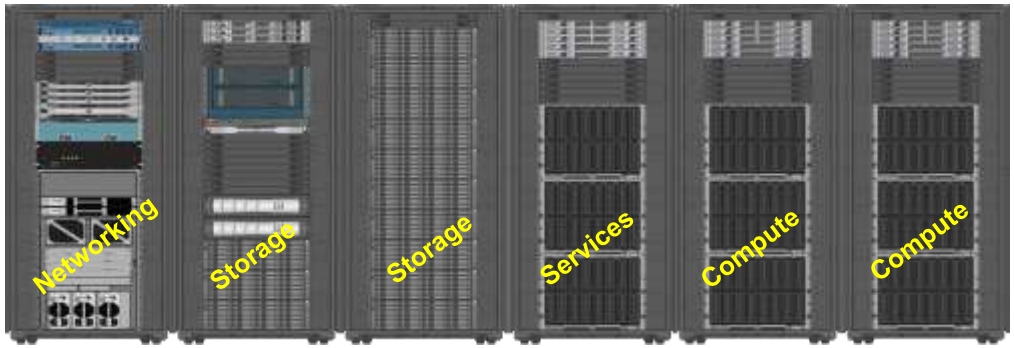
- **NCR supports a wide variety of cyber event types**
  - R&D testing
  - Product evaluation
  - Training events
    - System emulation
    - Target emulation
  - Mission rehearsal
  - Compliance testing
  - Risk reduction activities
  - Architecture analysis
  - OT&E
  - Malware analysis
  - Forensic analysis / Event Reconstruction

- **Over 90% Utilization in FY14**

Other Cyber Initiatives

Regional Service Delivery Points (RSDPs)

- RSDPs are intended to…
  - 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
  - support multiple classifications concurrently via MILS architecture
  - be a key component in the **enhanced network infrastructure**
- Deployment
  - Prototype used for continued development
  - Production RSDPs to be geographically dispersed
    - RSDP #1 homed to Army's Threat Systems Management Office (TSMO)
    - RSDP #2 to be deployed early FY15 (location TBD)
    - RSDP # 3 currently production



Provides Enterprise Resources for the Cyber Community

Cyber Range Interoperability Standards (CRIS) Working Group (WG)

- 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**

Enable Interoperability through Standardization

Questions?

AJ Pathmanathan
Arjuna.Pathmanathan.civ@mail.mil
571.732.2702