National Cyber Range

Prepared for ITEA Range Provider Panel Discussion

March 17, 2016

LOCKHEED MARTIN

Lori Pridmore
Director, Cyber Support Operations
lori.a.Pridmore@lmco.com

National Cyber Range – Background

- **Originally developed by Defense Advanced Research Projects Agency (DARPA) in the 2009-2012 timeframe**
- **Transitioned from DARPA to the DoD Test Resources Management Center (TRMC) in October 2012**
- **TRMC was charged with "operationalizing" the capabilities for use by the DOD test, training, and experimentation communities**

What is a Cyber Range?

Traditional "Ranges"

- Physical Environment for:
- Weapon Testing
- Live Training
- TTP Development, …
- Range Assets Change slowly

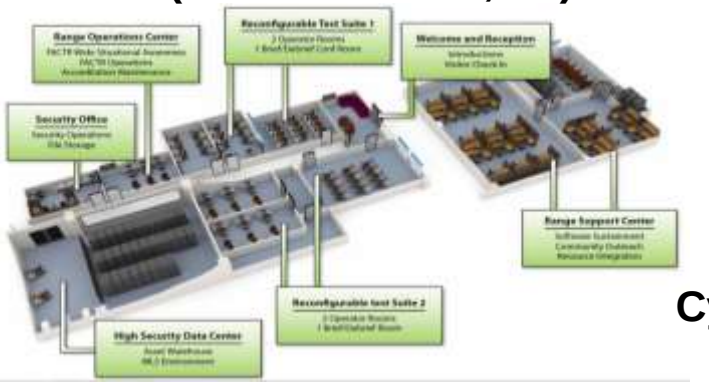
Cyber Range

- Place to Evaluate:
  - Effectiveness of Cyber Defenses
  - Effectiveness of Cyber Weapons
  - Train Cyber Warfighters
- Rehearse Mission
- TTP Development
- Range Assets Change Rapidly

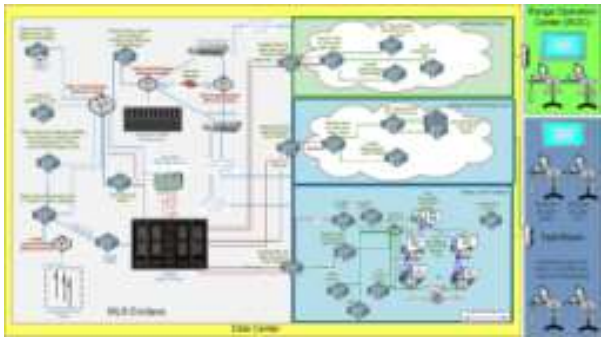
NCR provides a range solution that can span the entire spectrum of cyber test, evaluation & training needs

What is the National Cyber Range?

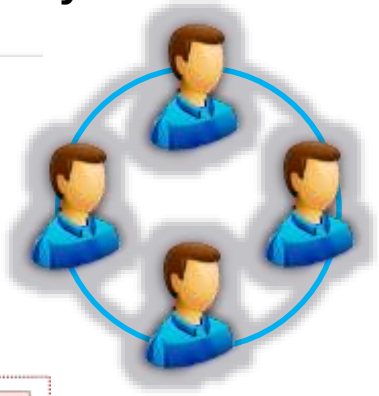
Computing Assets/Facility (LMCO Orlando, FL)



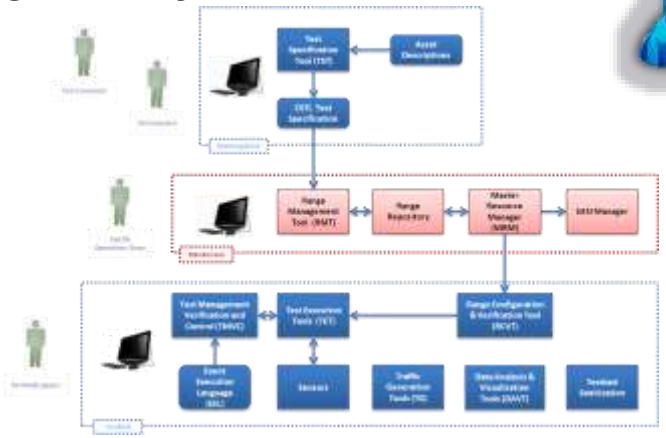
Encapsulation Architecture & Operational Procedures



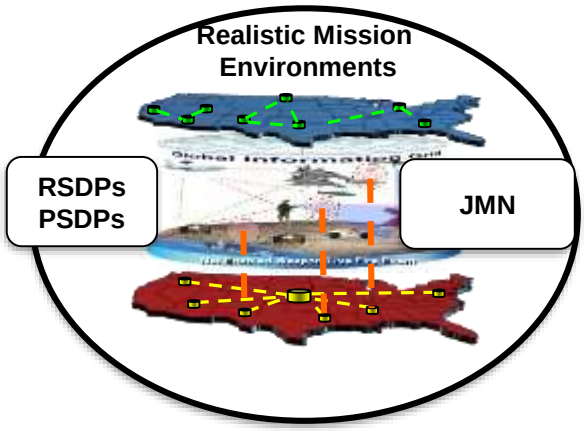
Cyber Test Team



Integrated Cyber Event Tool Suite



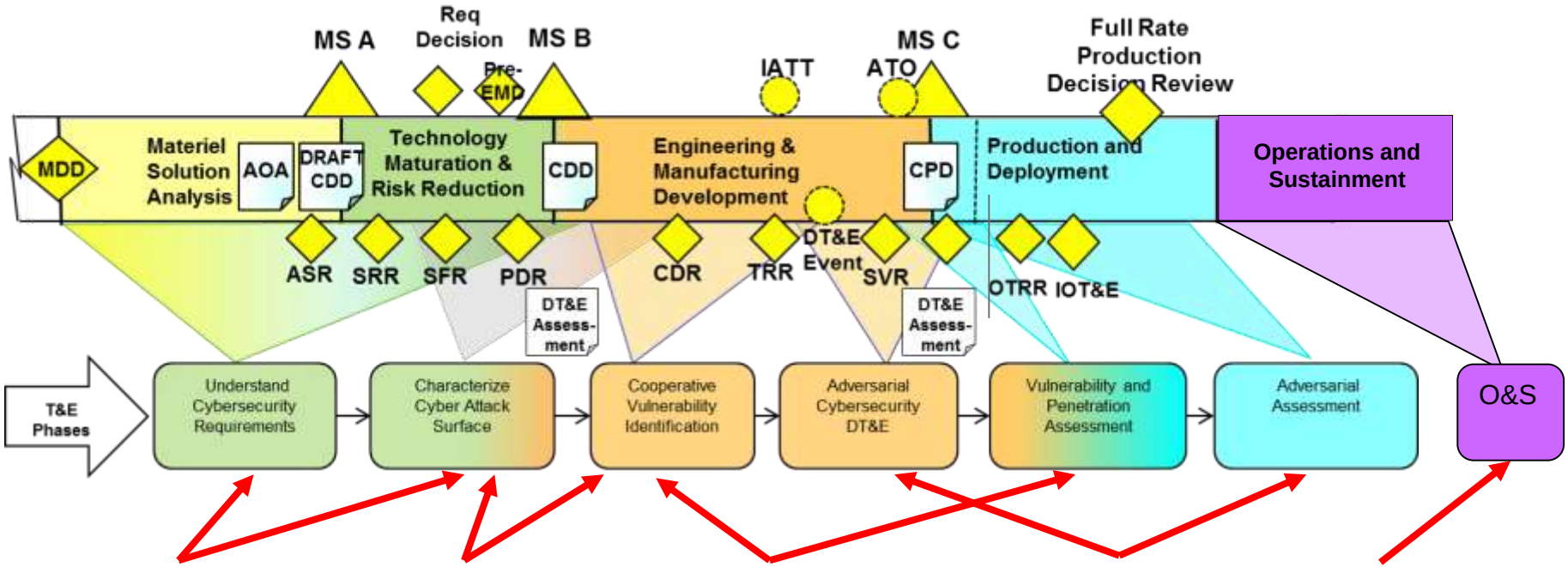
Secure Connectivity via JIOR and JMETC



NCR Key Capabilities

- **Multiple concurrent tests at varying classification levels are supported using a Multiple Independent Levels of Security (MILS) architecture**
  - Accredited for testing up to Top Secret / Sensitive Compartmented Information
  - Currently support up to 4 events at varying classification concurrently
- **Rapid emulation of complex, operationally representative network environments**
  - Can scale up to ~40K high-fidelity virtual nodes
  - Red/Blue/Gray support, including specialized systems (e.g., weapon systems)
- **Automation provides significant efficiencies that enable more frequent and more accurate events**
  - Reduces timelines from weeks or months to hours or days
  - Minimizes human error and allows for greater repeatability
- **Sanitization to restore all exposed systems to a known, clean state**
  - Allows assets to be reused even when they are exposed to the most malicious and sophisticated uncharacterized code
- **Supports a diverse user base by accommodating a wide variety of event types (R&D, OT&E, information assurance, compliance, malware analysis, etc.) and communities (testing, training, research, etc.)**

When To Use a Cyber Range?
Across the Acquisition Life Cycle



Pre MS A/B
Requirements and Systems Security Engineering Analysis

NCR Event
Cybersecurity Architecture Evaluation

SE/DT&E
Evaluate Software and Systems Security Architecture

NCR Event
Cybersecurity Verification and Validation

RMF/DT&E
Verify Baseline Cybersecurity Requirements and Vulnerability Assessment

NCR Event
Mission Thread Testing with Blue Team

DT&E/OT&E
Evaluate Mission Capabilities and Interoperability in a Contested Environment

NCR Event
Mission Thread Testing with Red Team in a Realistic Threat Environment

Training & Exercises
Evaluate TTPs in a Contested Environment

NCR Event
Large-scale Simulation to Train Cyber Mission Forces and Evaluate Cyber Defensive and Offensive Operations

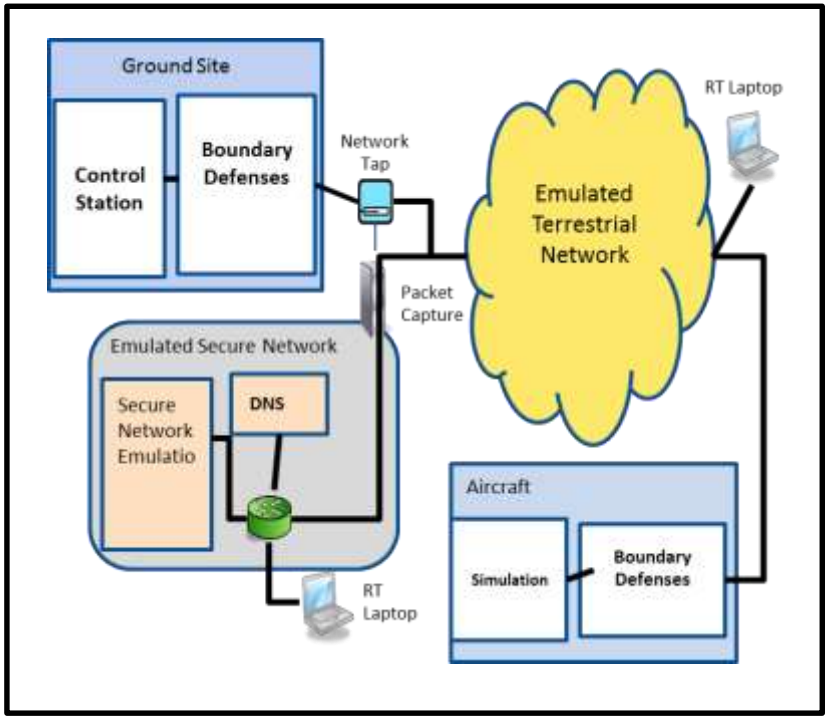
What You Can Do With the NCR (1 of 2)

Question: Will my architecture scale in the field?

- Will it handle the expected user load?
- What are potential issues that can only be discovered at scale (normally only found very late in the testing process)

What you get:

- Minimize unexpected performance failures late in the DT or early OT process
- Reduce costly rework
- Empirical data to show whether or not the system operates as predicted in a realistic environment



Will this architecture scale to support the mission?

Results provide insight into system performance before the design is finalized

What You Can Do With the NCR (2 of 2)

Question : How do I generate realistic cyber mission effect within a large scale training exercise safely and securely?

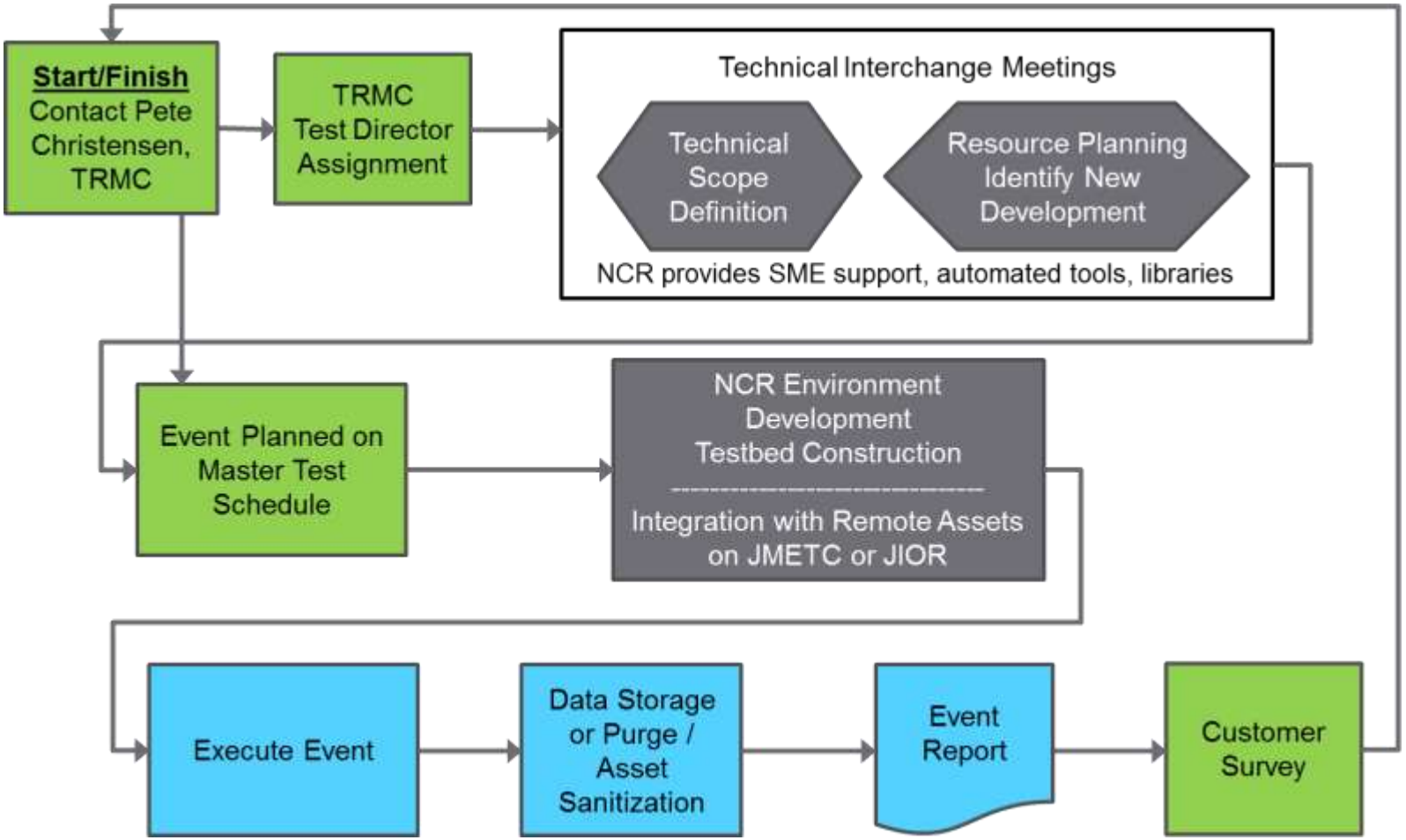
- OCO is destructive
- Cyber weapons and TTPs are often classified at security levels higher than the rest of the exercise

What you get:

- Realistic operator training
- Repeatability to evaluate relative effectiveness of multiple TTPs
- On-demand, low-cost evolution of the environment to represent salient real-world environments

A safe environment for safely conducting realistic cybersecurity training

How to get engaged



Summary

- Cyberspace threats to DoD systems are proliferating at an unprecedented rate
  - Leadership has recognized that current cybersecurity testing and training needs further improvements
  - Leadership is placing increased emphasis on the need to consistently incorporated realistic cybersecurity testing and training at all levels and phases
  - Early identification of system vulnerabilities can make them easier and cheaper to fix
- NCR provides customers with a unique set of cybersecurity test, evaluation, and training capabilities
  - NCR enables acquisition organizations to conduct system specific cybersecurity test and evaluation events that are tailored to meet program requirements throughout the systems acquisition lifecycle
  - NCR enables operational organizations to conduct realistic cybersecurity training in environments that closely replicate the real world
- NCR capabilities have been independently validated and have successfully supported a wide variety of cyber events including
  - Developmental Testing
  - Operational Testing
  - Training/Exercise
- NCR is institutionally funded and cost effective
  - Customers only pay for their own personnel, travel, systems under test, special equipment, etc.