



The National Cyber Range: A Systems Engineering Resource for Cybersecurity R&D, S&T, Testing and Training

Prepared for the 18th Annual Systems Engineering Conference

October 27 and 28, 2015

Presented by: **Pete Christensen, Director, National Cyber
Range**

peter.h.Christensen.civ@mail.mil

571-372-2699



What, Why, How?

- **What do we want to accomplish?**

- Provide an overview of T&E Policy and Guidance
- Provide an overview of the National Cyber Range (NCR)
- Discuss how programs and organizations can benefit from using the NCR

- **Why is this important?**

- Cyberspace Threats are proliferating
- Systems Security Engineering (SSE) and Risk Management Framework (RMF)
- Recent policies are emphasizing the importance of increased realism in cybersecurity testing and training
- TRMC and the NCR can help!

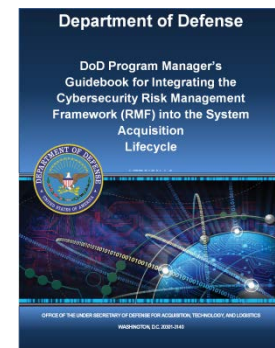
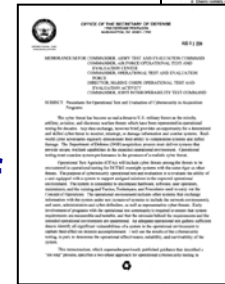
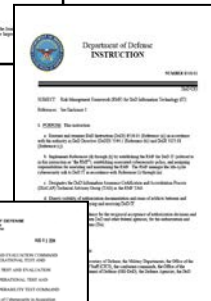
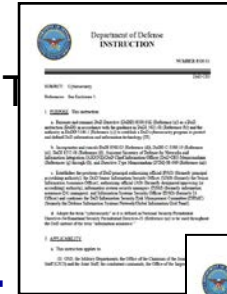
- **How will we do it?**

- Cover some existing DoD cybersecurity guidance and policies
- Explain some of the history behind the NCR
- Provide an overview of NCR technical capabilities
- Discuss what you can do with the NCR and types of events that it supports
- Describe NCR event planning and how customers can get engaged



New/Ongoing Cybersecurity Policy and Guidance Activities

- **Revision of DoDI 5000.02: Issued 6 Jan 2015**
 - New/better guidance for both developmental and operational testing of IT
- **Revision of DoD 8500.01, Cybersecurity: 14 Mar 2014**
 - Expanded scope and specificity
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: 14 Mar 2014**
 - Provides policy, clarity and guidance on the RMF and compliance
- **Six Phase Cybersecurity T&E Process: Planned Aug 2015**
Incorporated into Defense Acquisition Guidebook Chapter 9
- **OSD DOT&E- Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: 01 Aug 2014**
 - Formalizes OT&E Phases
- **Cybersecurity Implementation Guidebook for PMs: In Draft**
 - Address Cybersecurity T&E across the acquisition lifecycle
- **Cybersecurity T&E Guidebook: Issued July 2015**
 - Address Cybersecurity T&E across the acquisition lifecycle

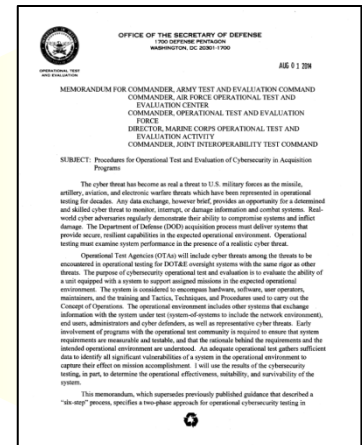
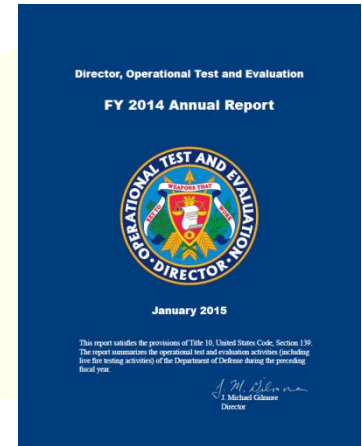




DoD Cybersecurity Test Posture and Emerging Requirements

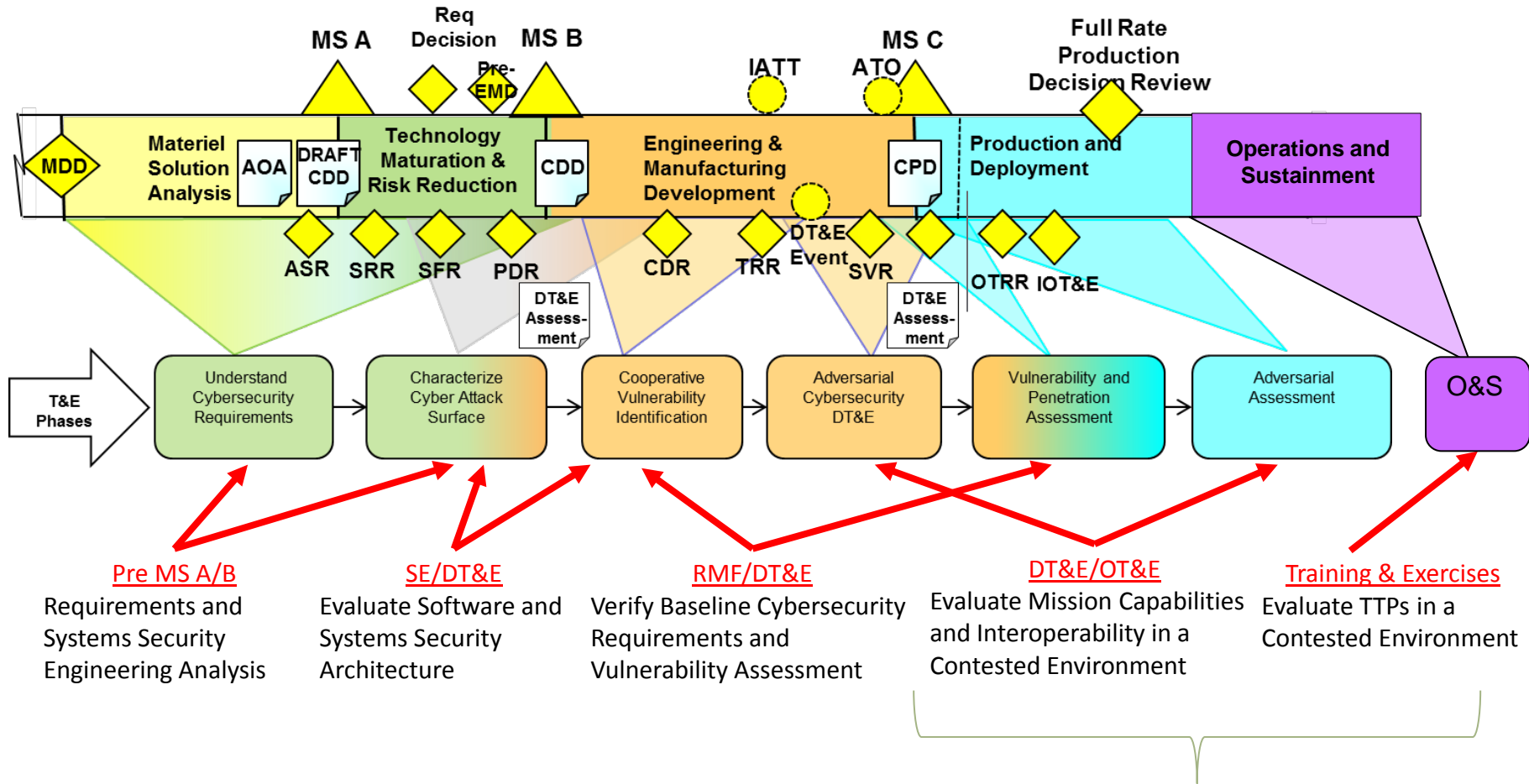


- “Also in 2014, my office conducted 16 cybersecurity assessments in conjunction with Combatant Command and Service exercises...Despite the improved defenses, my office found that at least one assessed mission during each exercise was at high risk to cyber-attack from beginner to intermediate cyber adversaries.”
- **“DOT&E found significant vulnerabilities on nearly every acquisition program that underwent cybersecurity OT&E in FY14.”**
- “The cyber threat has become as real a threat to U.S. military forces as the missile, artillery, aviation, and electronic warfare threats which have been represented in operational testing for decades.”
- “Operational Test Agencies (OTAs) will include cyber threats among the threats to be encountered in operational testing for DOT &E oversight systems with the same rigor as other threats.”
- **“All oversight systems capable of sending or receiving digital information are required to conduct cybersecurity testing.”**





Cybersecurity T&E “Shift Left” – Six Phased Process



OT Focus – Codified in OSD
DOT&E Memo dated 01 Aug 2014



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

National Cyber Range
Adaptable, multi-dimensional, heterogeneous cyber test environment
The Nation's environment for cyber research

The National Cyber Range is the measurement capability providing a realistic quantifiable assessment of the Nation's cyber research and development technologies, enabling a revolution in national cyber capabilities and accelerate transition of these technologies

The National Cyber Range will allow classified and unclassified researchers to measure their progress ...
... in either a classified or unclassified environment,
... against appropriate threats with sufficient timeliness and accuracy,
... to allow corrections and needed new capabilities to be determined.

Leap-ahead research and quantifiable assessment of cyber tools, processes and architectures facilitates;
Revolution in national cyber capabilities
Rapid technology development
Accelerated deployment

Providing the environment to solve the Nation's Cyber problems
Unconstrained cyber research environment supporting the CNOI
Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

What is the National Cyber Range?
A dedicated cyber testbed to enhance the Nation's ability to defend against cyber attacks

The National Cyber Range will

A cyber test center to:

- ✓ Enable leap-ahead advances to defend and exploit the cyber realm
- ✓ Enable revolutionary cyber testing

The National Cyber Range will

- Provide a dedicated "test bed" to produce qualitative and quantitative assessments of the security of cyber technologies and scenarios.
- Provide a revolutionary, safe, instrumented environment for our national cyber security research organizations to test the security of information systems.
- Revolutionize the state of the art of cyber security testing.

Revolutionary test technologies

- Automated configuration, sanitization, reconfiguration
- Automation
- Virtualization technology
- Scale
- Simulate human activity
- Realism
- Time dilation & contraction
- Efficiency
- All systems wired, MARKET, control systems, phone, etc.
- Completeness

Facilitates continuous, realistic, verifiable testing

What is a Cyber Range?

Traditional "Ranges"

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



Cyber Range

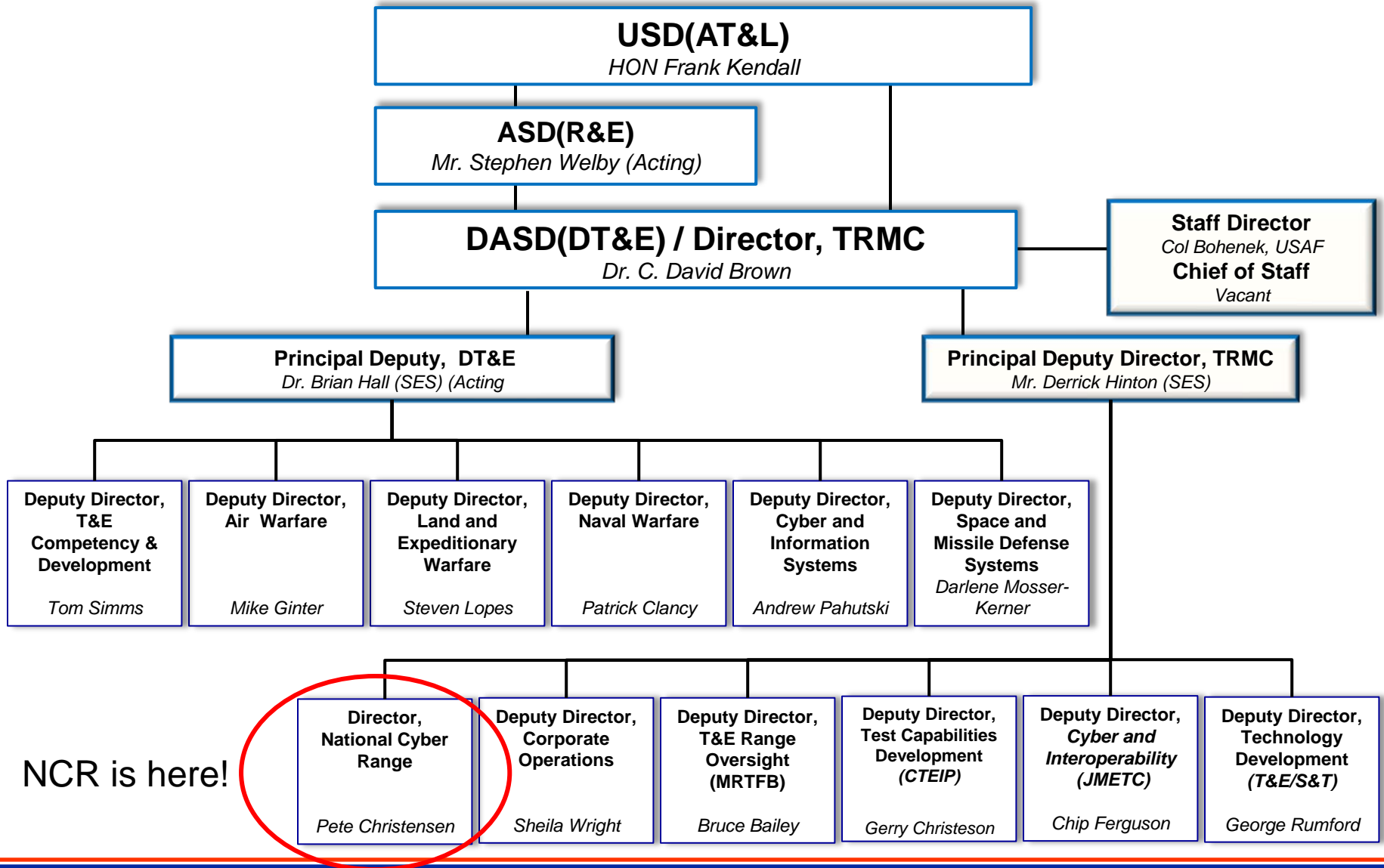
- Place to Evaluate:
 - Effectiveness of Cyber Defenses
 - Effectiveness of Cyber Weapons
 - Train Cyber Warfighters
- Rehearse Mission
- TTP Development
- Range Assets Change Rapidly



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



DASD(DT&E) / Director, TRMC



NCR is here!



NCR – Vision and Mission

- **Vision**

- Be recognized as the cyberspace test range of choice for providing mission tailored, hi-fidelity cyber environments that enable independent and objective testing and evaluation of advanced cyberspace capabilities

- **NCR Mission Statement**

- Provide *secure facilities, innovative technologies, repeatable processes, and the skilled workforce*
- Create *hi-fidelity, mission representative cyberspace environments*
- Facilitate the integration of the cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, DHS, industry, and academia

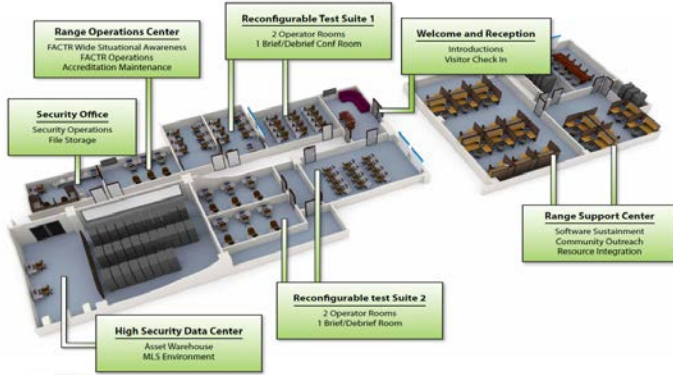


BLUF – NCR Key Capabilities

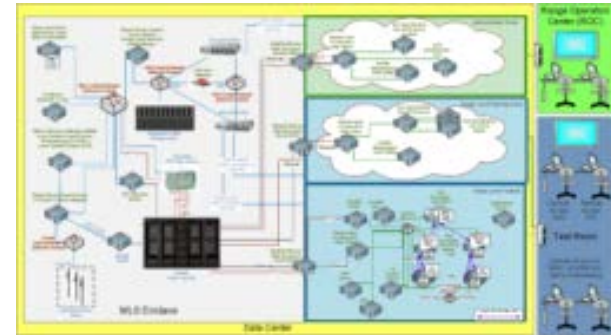
- **Multiple concurrent tests at varying classification levels are supported using a Multiple Independent Levels of Security (MILS) architecture**
 - Accredited for testing up to Top Secret / Sensitive Compartmented Information
 - Currently support up to 4 events at varying classification concurrently
- **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.)**

What is the National Cyber Range?

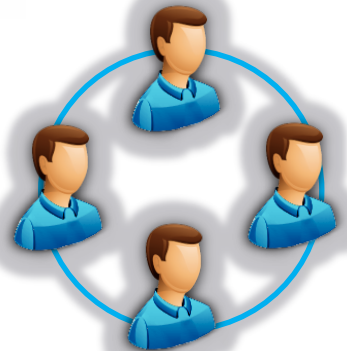
Computing Assets/Facility (LMCO Orlando, FL)



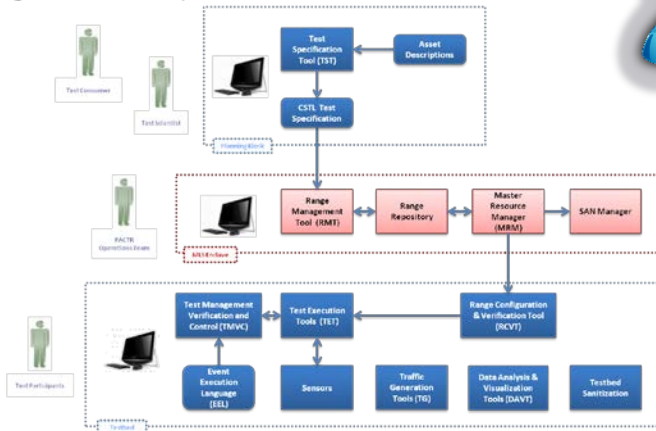
Encapsulation Architecture & Operational Procedures



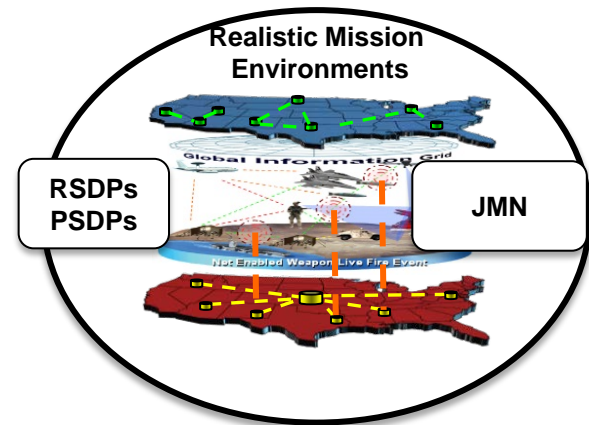
Cyber Test Team



Integrated Cyber Event Tool Suite

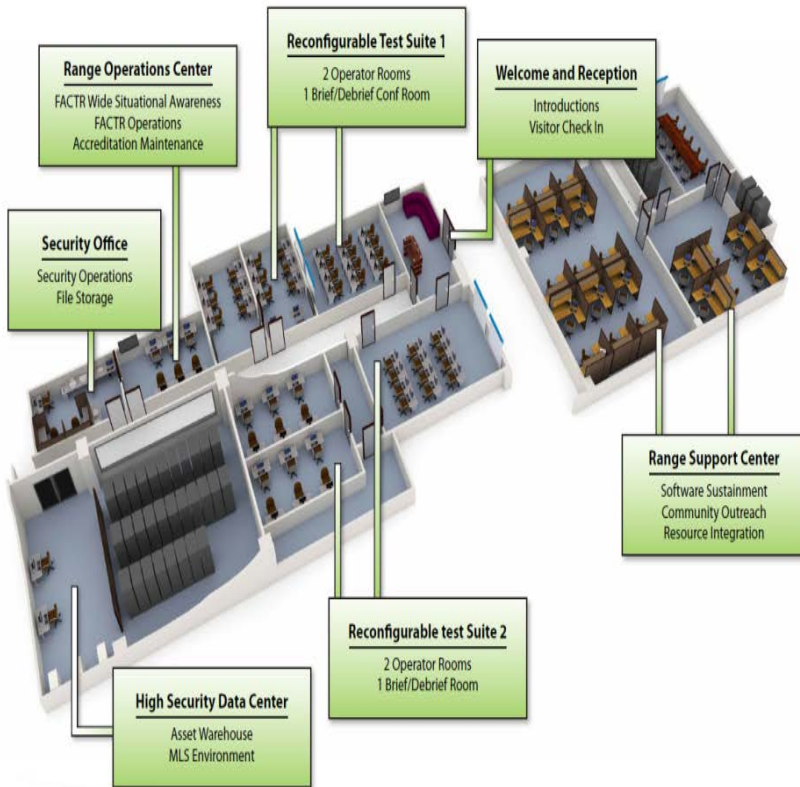


Secure Connectivity via JIOR and JMETC





Facility Overview: On-site or Remote Access



- Fully accredited SCIF
- Supports at least two independent concurrent events on-site
- Test suites can be utilized at different security levels and contain:
 - Two test rooms
 - Conference room
- Unclassified Range Support Center
- Wireless Testing Environment

- Remote access currently provided through the Joint IO Range (JIOR) and JMETC MLS

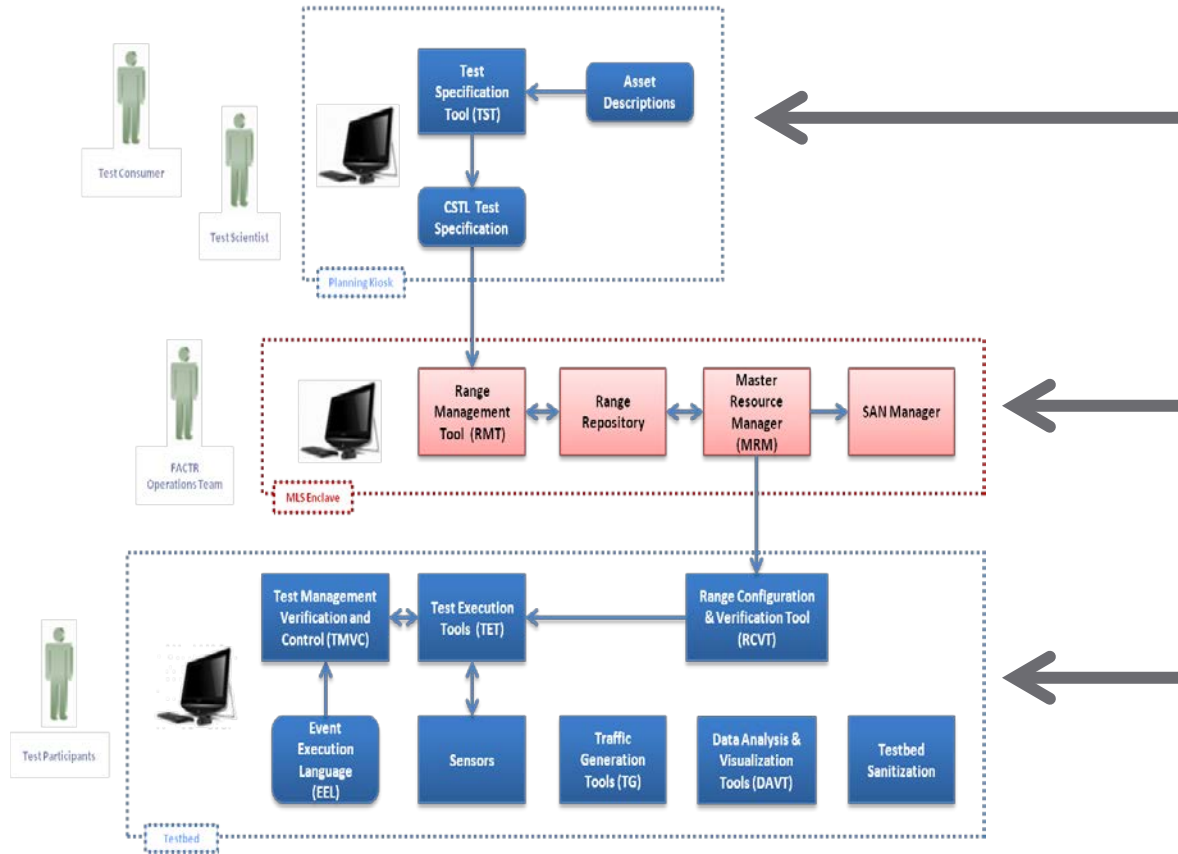


Facility Overview: Support for Wireless Testing



- **Wireless environment that supports classified testing (TS/SCI)**
- **Support for mobile computing: iOS, Android, Windows 8 on tablets, cell phones, and multimedia devices**

Automation Toolkit: End to End Support



Tools to support event planning

Tools to define and manage resource requirements

Tools to automatically:

- Build, verify and sanitize your environment
- Support event execution

Faster, more reliable, event environment creation and execution



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

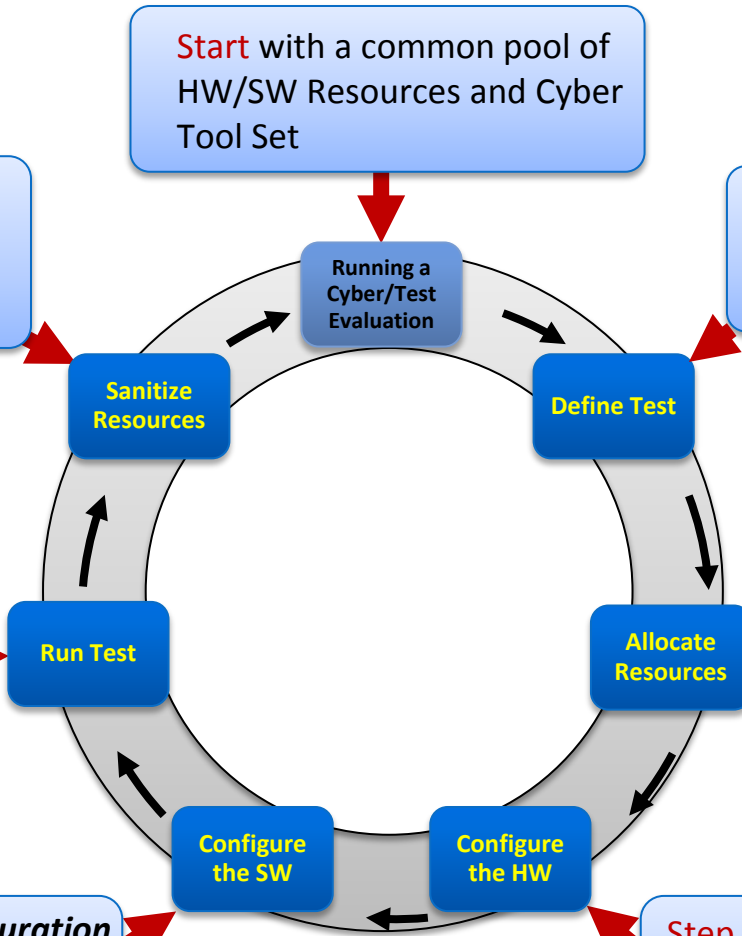
Step 6: **Sanitization Tool** sanitizes HW and “virtually” puts HW resources back in pool

Step 2: **Resource Allocation** determines what resources from the pool are needed and allocates them to Event

Step 5: **Test Execution Tools** are used by the event team along with event-specific systems for execution and data collection/analysis

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

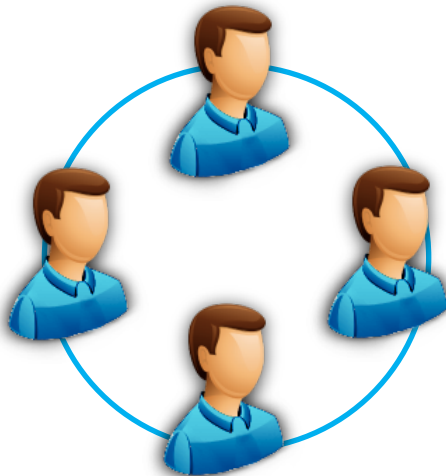
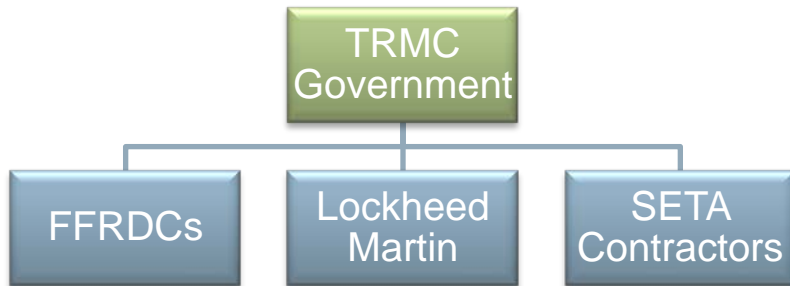
Step 4: **Range Configuration (ACORN)** tools automatically configure the SW you need to run the event





Cybersecurity T&E “As A Service”

ONE NCR TEAM



- **Services Include, But Are Not Limited To:**

- End-to-End Test Support
- Test Bed Design Support
- Cyber and Testing Expertise
- Threat Vector Development
- Custom Traffic Generation
- Custom Sensor and Visualization Support
- Custom Data Analysis
- Integration of Custom Assets
 - Software
 - Hardware
 - Wired and Wireless
 - Remote Red/Blue Team Support

The NCR's Most Valuable Resource Is A Diverse and Experienced World Class Cybersecurity Workforce

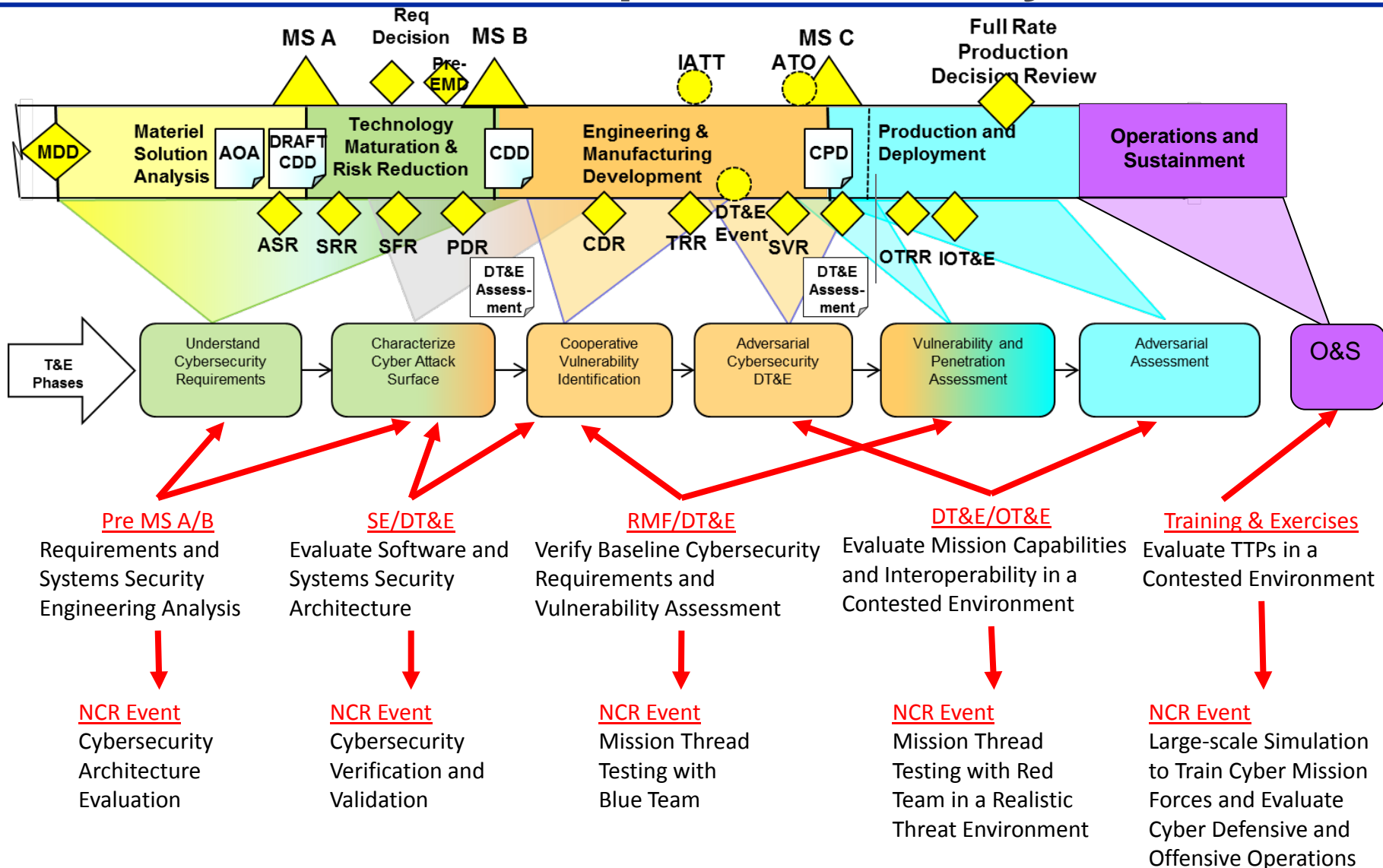


Why Use a Cyber Range?

- Requirements to **conduct testing that cannot or should not occur on open operational networks due to potential catastrophic consequences**, for example full execution of extremely malicious threats on realistic representations of systems and networks (e.g., releasing self-propagating malware)
- Requirements to **test advanced cyberspace tactics, techniques, and procedures that require isolated environments of complex networked systems** (e.g., movement on the Internet)
- The need to **rapidly and realistically represent operational environments at different levels of security, fidelity, and/or scale** (e.g., Blue [friendly] force, Red [adversary] force, and Gray [neutral] networks)
- The need for **precise control of the test environment that allows for rapid reconstitution to a baseline checkpoint, reconfiguration, and repeat of complex test cases**; this would include the need for rapid variation of conditions to quickly evaluate hundreds of scenarios



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



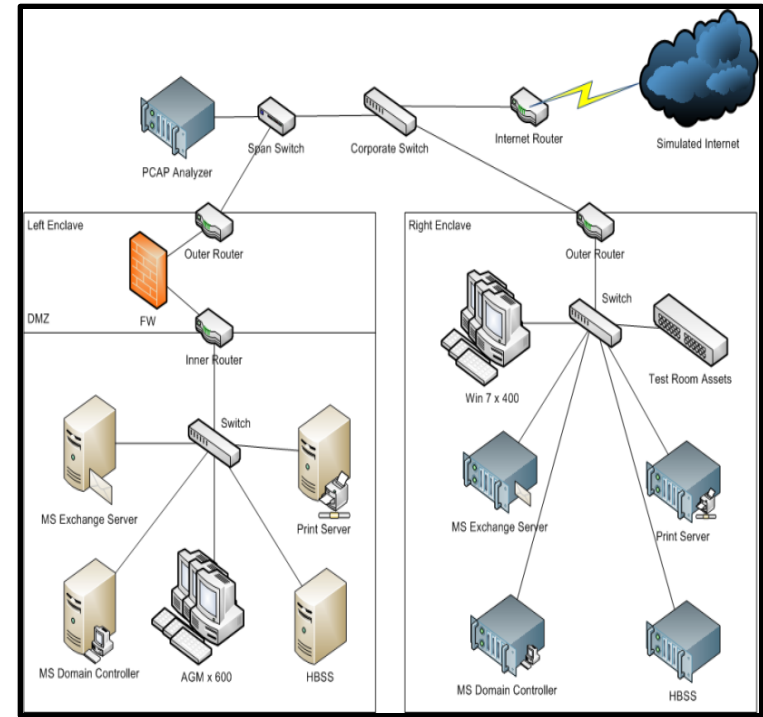
What You Can Do With the NCR (1 of 4)

Question: Does Product “A” close a requirements gap?

- Does it mitigate a particular set of threats within my operational system?
- How well?
- What is my residual risk?

What you get:

- Empirical evidence showing how the technology or product closes the requirements gap in your operational environment



How does adding a technology to my existing environment reduce my threat surface?

Commercial Product / Emerging Technology Evaluation

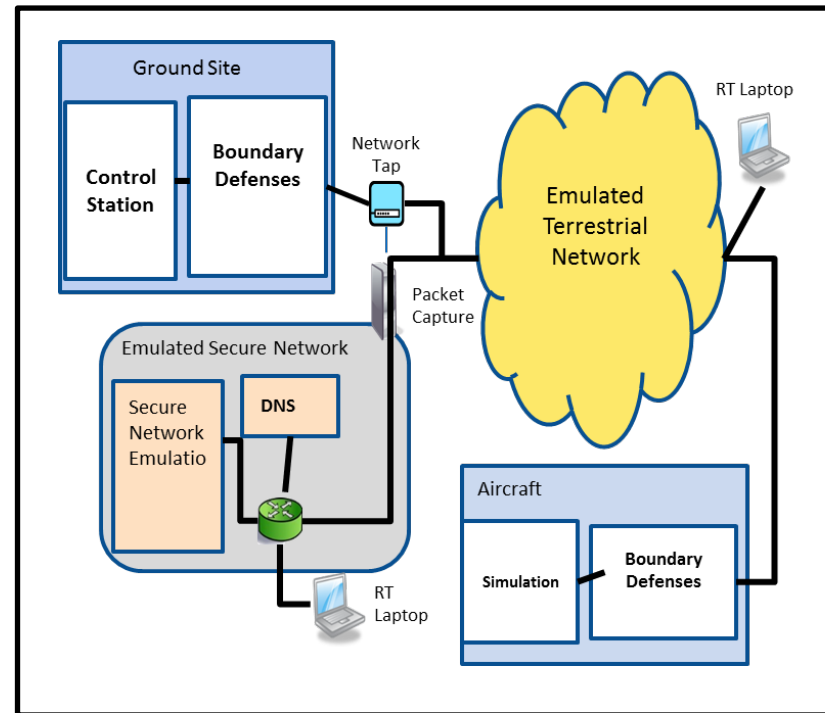
What You Can Do With the NCR (2 of 4)

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 (3 of 4)

Question: How resilient is my system to cyber attacks and faults when connected into the overall system of systems?

- System is a distributed sensing system that has a dependency on an external service to interconnect platforms to ground stations
- How does my system behave when there are problems with external systems?

What you get:

- Increased resilience to cyber attack and failures
- Reduce costly rework
- Empirical data to show whether or not the system operates as predicted in a realistic environment
- Understand how the dependencies on the broader DoD environment affect the ability to meet the mission



System Testing During Development

What You Can Do With the NCR (4 of 4)

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

Be able to use unrestricted TTPs

Operate on realistic and complex network topologies



Integrate home base and remote training

Have access to interactive web sites

A safe environment for safely conducting realistic cybersecurity training



NCR Supports Many Different Types of Events



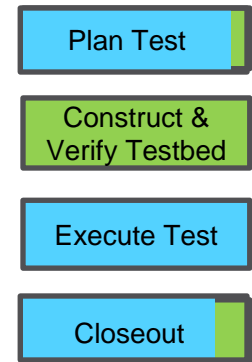
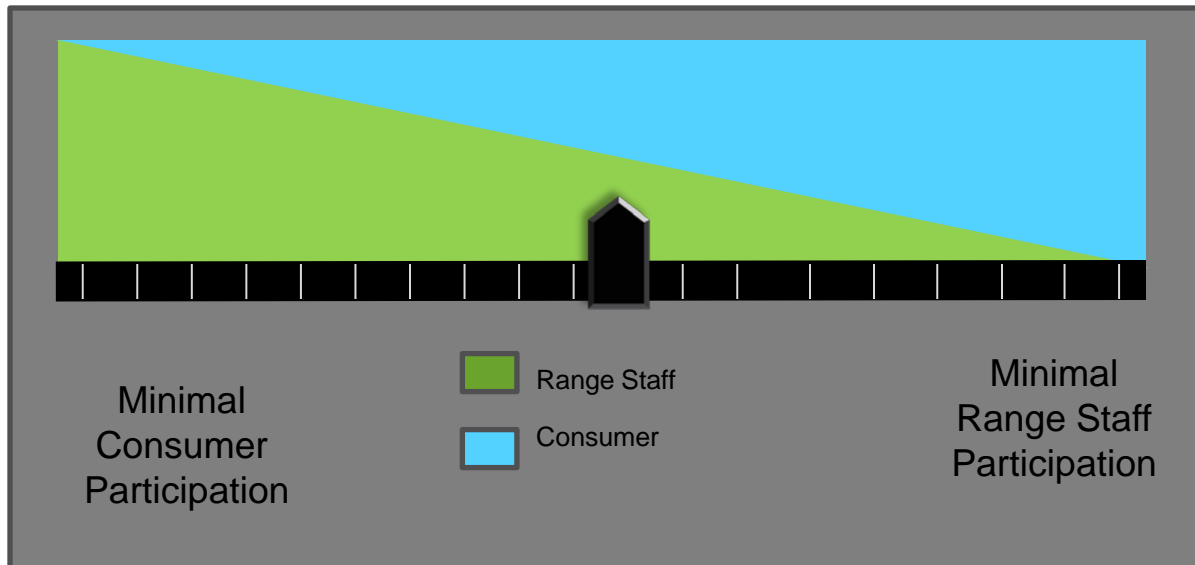
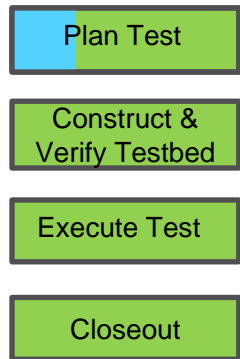
- **NCR supports a wide variety of cyber event types**
 - R&D testing
 - Product evaluation
 - Training events
 - System emulation
 - Target emulation
 - Mission rehearsal
 - Risk reduction activities
 - Architecture analysis
 - DT&E
 - OT&E
 - Malware analysis
 - Forensic analysis
- **Events can occur exclusively at NCR, or in conjunction with other Joint Mission Environment Test Capability or Joint Information Operations Range nodes**
- **Level of support from NCR is dependent on customer needs**



NCR Operational Support Models

We work with consumer to define tests and then NCR personnel do everything else with periodic review.

We deliver a verified range and support sanitization at end & consumer does everything else.



You Select the Desired Level of Support from NCR Staff



NCR Planning and Scheduling Procedures



- **NCR Director:**
 - Coordinates with the JMETC PM to review schedules and make decisions
 - Owns the NCR Event Planning List and the NCR Range Schedule
- **The NCR Event Planning List describes the events that are currently in the discussion/planning phase and scheduled but not yet run**
- **NCR Range Schedule describes the events to be held on the range**
- **Monthly Review held to:**
 - Formally add/move events to the schedule
 - Review customer feedback on tests
 - Review Event Planning Port



NCR Event Planning Stages

- **Event Pre-Planning & Planning**

- Discussions
- Use Case Development

- **Event Design**

- Goals, Objectives & Assumptions
- Outputs & Data Collection Plan
- Environment Design

- **Event Development**

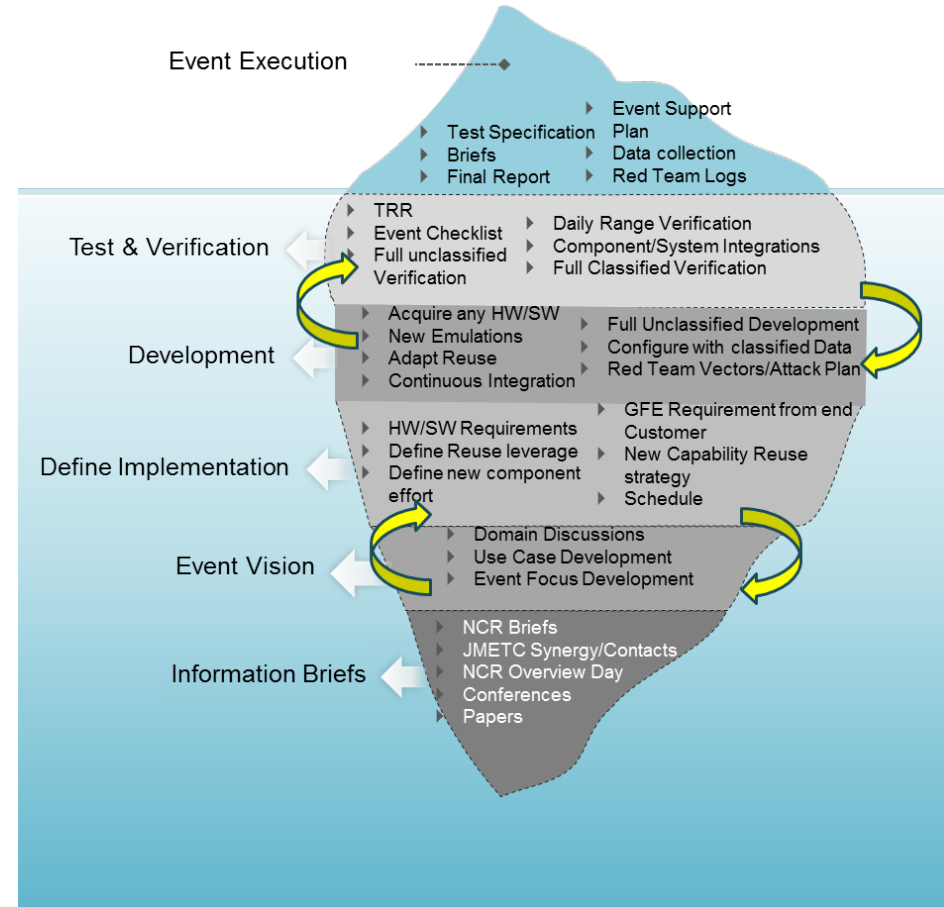
- Red Team Operations
- Environment Build & verification

- **Event Execution**

- Conduct tests and data
- Review results & adapt as needed

- **Event Completion**

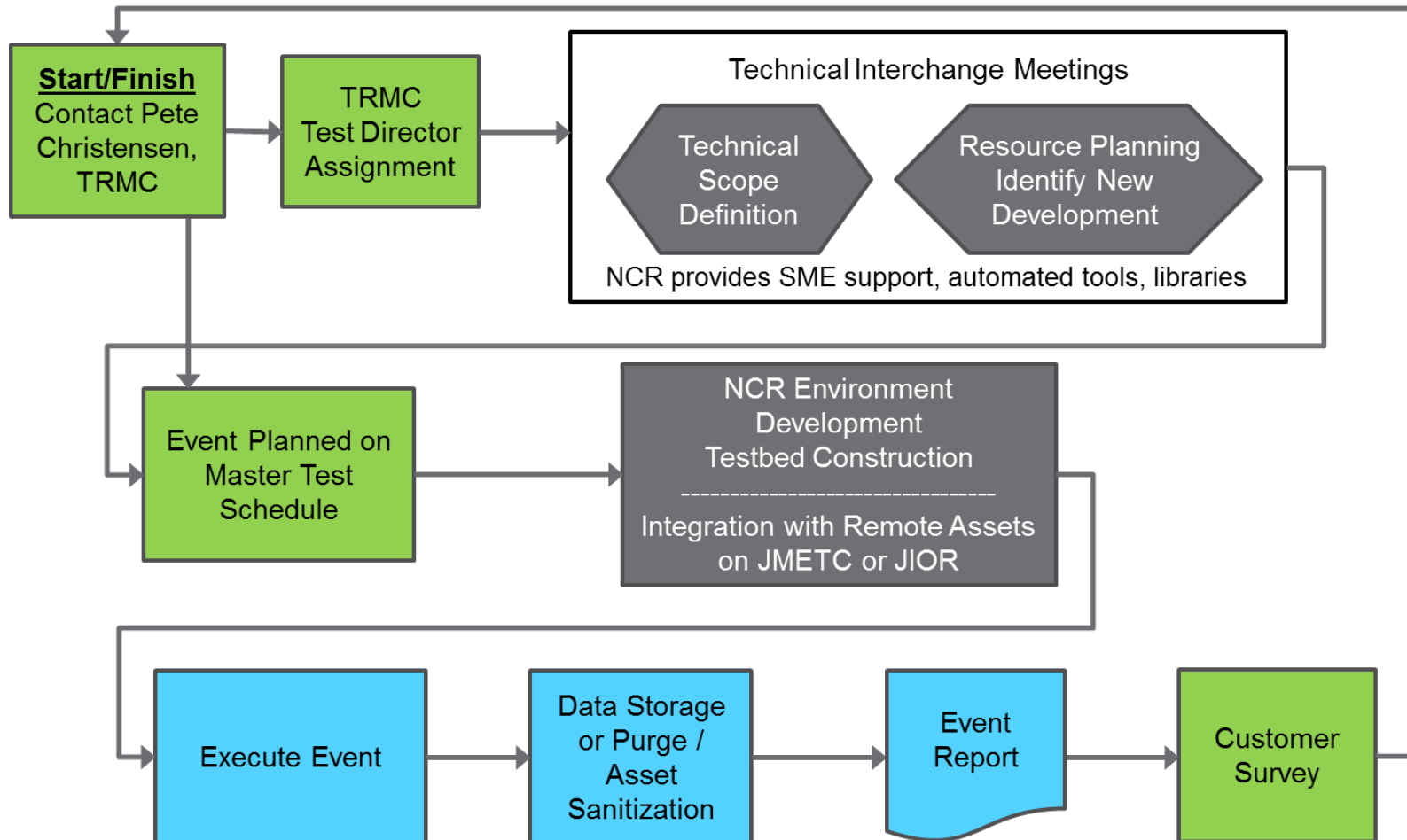
- Data Analysis
- Reporting, Briefings, Next Event Planning



Example Generalized from Actual NCR Event



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 incorporate 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.



Questions?

Peter H. Christensen

Director, National Cyber Range

TRMC Office Phone: 571-372-2699

TRMC Email: peter.h.christensen.civ@mail.mil

Address:

4800 Mark Center Drive

Suite 07J22

Alexandria, Va. 22350