Test Resource Management Center and the National Cyber Range

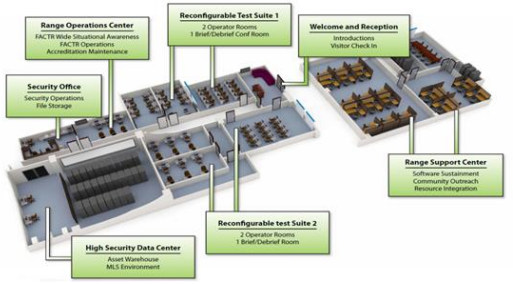
07 March 2017
Prepared for
32nd Annual National Test & Evaluation Conference
Strategic T&E Collaboration: Government & Industry Partnering to Achieve Decisive Operational Advantage

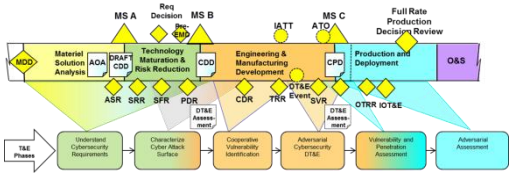
Prepared by
National Cyber Range and the NCR Team
Peter.H.Christensen.civ@mail.mil
571-372-2699

Cleared for Public Release
01 March 2017 Case # 17-S-1016

What, Why, How?

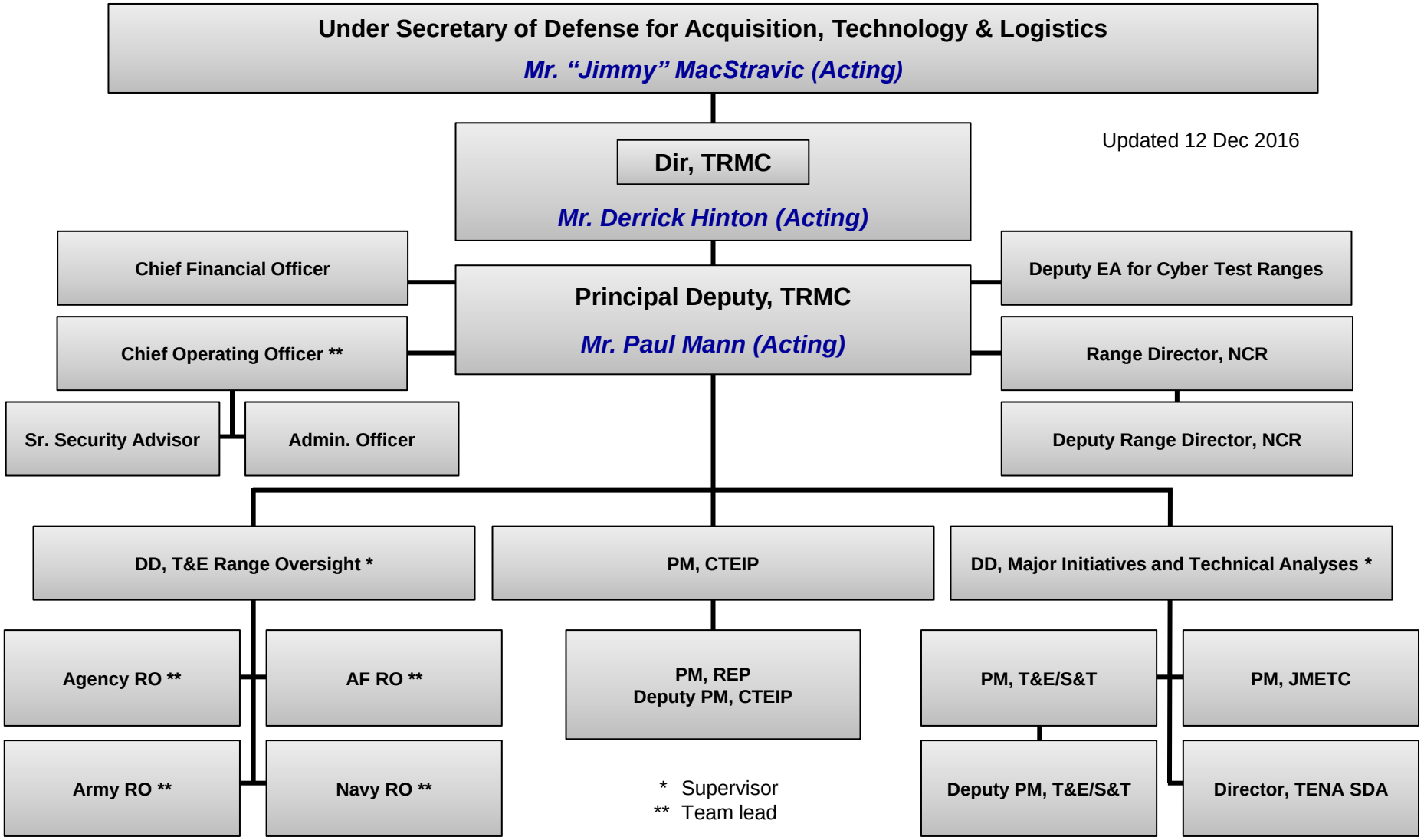
- What do we want to accomplish?
  - Provide an introduction to the NCR and the supporting Team
- Why is this important?
  - TRMC/NCR provides Cybersecurity Testing and Training as a service for DOD Customers
  - NCR has been recognized by DOD and Industry for excellence
- How will we do it?
  - Describe TRMC Organization
  - Provide background behind new Policy and Approaches for Cybersecurity T&E
  - Highlight some NCR capabilities and usage in support of Testing and Training Customers
  - Share Lessons Learned and Pathfinder Initiatives





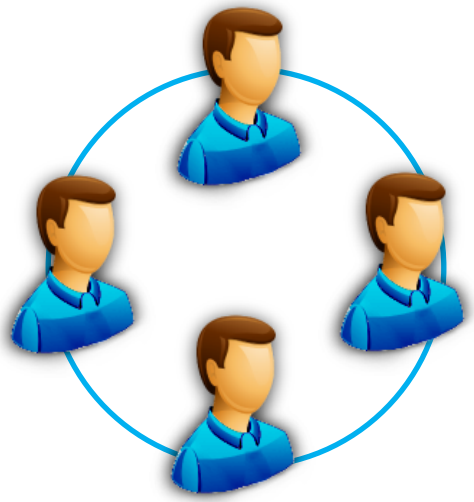
AVIATION WEEK
Executive
INTELLIGENCE

TRMC Organization



TRMC Provides Cybersecurity T&E Ranges and Services

ONE TRMC TEAM



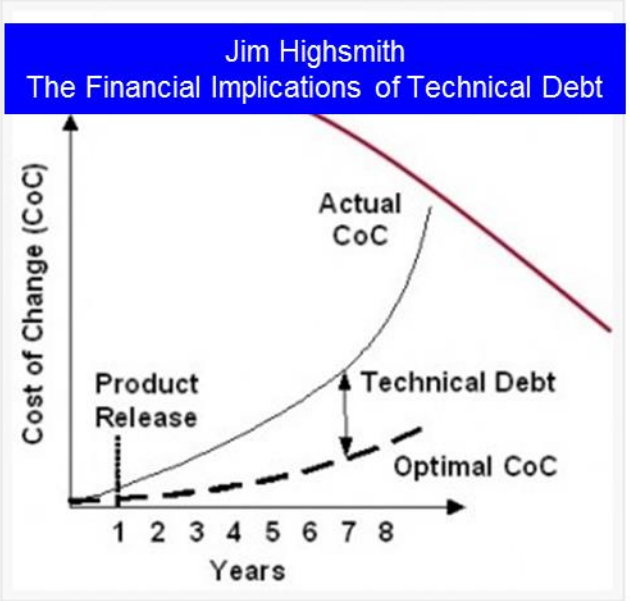
- **Services Include, But Are Not Limited To:**
  - End-to-End Test Support
  - Test Bed Design Support
  - Cyber and Testing Expertise
  - Threat Vector Development
  - Custom Traffic Generation
  - Custom Sensor and Visualization Support
  - Custom Data Analysis
  - Integration of Custom Assets
    - Software
    - Hardware
    - Wired and Wireless
    - Remote Red/Blue Team Support

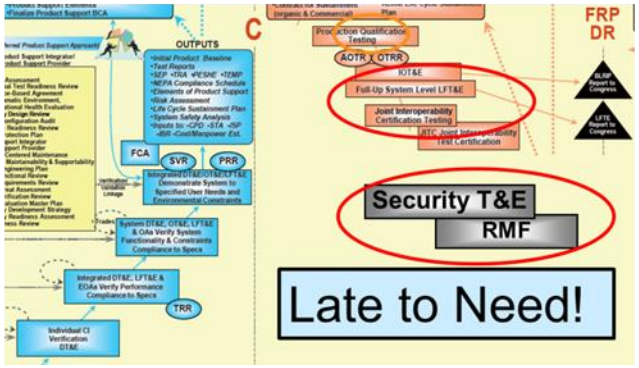
Customers Identify Cyber T&E Requirements to TRMC Government NCR Team provides people and resources to satisfy them!

Historically: DOD Cyber Practices Have Created Technical Debt!

- Technical Debt: Cost of work that must be accomplished before a job can be completed
  - Type 1 Debt: Unintentionally incurred: consequence of flawed design or implementation
  - Type 2 Debt: Intentionally incurred: Organization makes a decision to optimize for the present rather than for the future

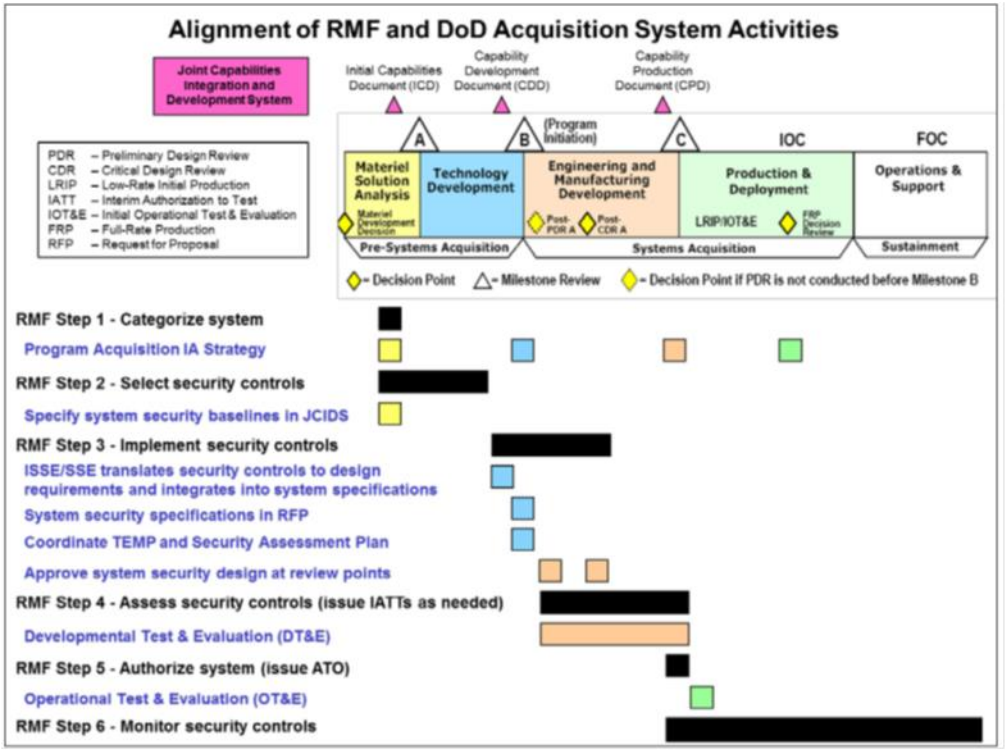
- Historically DOD Cybersecurity processes create “Technical Debt”
  - Type 1: Cybersecurity Requirements definition and SSE processes poorly executed
  - Type 2: Controls Verification deferred until just prior to Initial Operational Test and Evaluation





DOD Shift Left Initiatives are Intended to Reduce Technical Debt!

Controls Compliance and Verification Necessary but Not Sufficient!



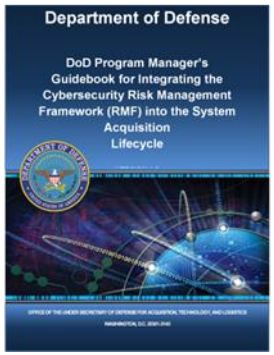
Graphics Source: DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

Security Controls Assessment verifies compliance…
Necessary and Not Sufficient!

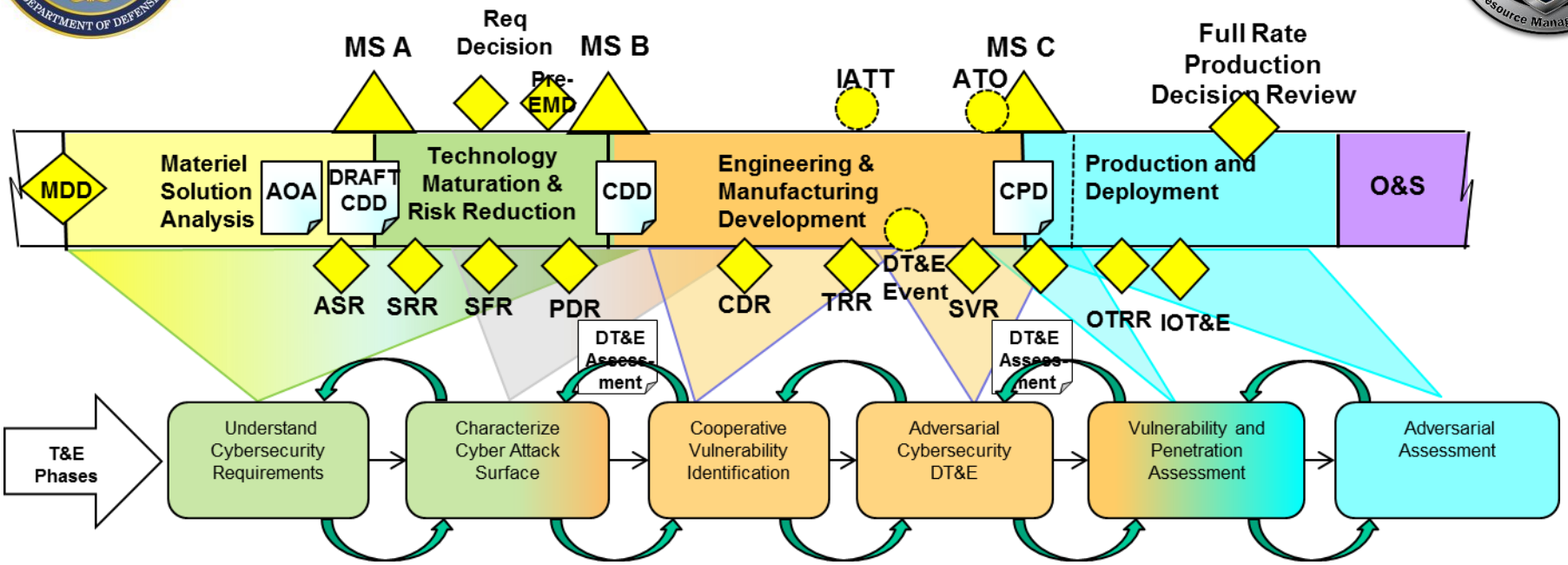
New/Ongoing Cybersecurity Policy and Guidance Activities

- DoDI 5000.02: Issued 6 Jan 2015
  - New guidance for both developmental and operational testing of IT
- 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
- OSD DOT&E- Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: 01 Aug 2014
- Cybersecurity Implementation Guidebook for PMs: Issued 26 May 2015
  - Address Cybersecurity T&E across the acquisition lifecycle
- Cybersecurity T&E Guidebook: Issued July 2015
  - Provides detail for practical application
- DTM 17-001 – Cybersecurity in the Defense Acquisition System: 11 Jan 2017



Guidance and Policy Will Not Make Us "Cyber Secure"!

Iterative Cybersecurity T&E Reduces Technical Debt/Manages Mission Risk



- Phases are iterative and incremental!
  - Initial Phases reduce Type 1 Debt!
    - Complements System Security Engineering and Risk Management Framework SE and RMF Activities
  - Later Phases reduce Type 2 Debt!
    - Promotes Understanding of Mission Risk!

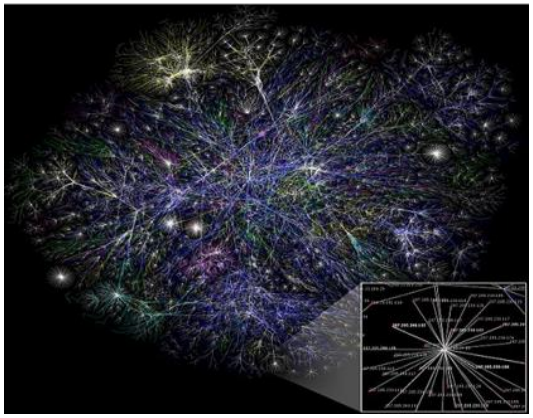
RMF Manages Program Risk….Cybersecurity T&E Manages Mission Risk

What is a Cyber Range vs. Traditional Range?

Traditional "Ranges"

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

Graphic Source: WIKIPEDIA Commons



Cyber Range

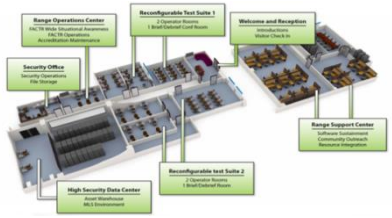
- Place to create "Cyberspace Environments" to evaluate:
  - Effectiveness of Cyber Defenses
  - Effectiveness of Cyber Weapons
  - Train Cyber Warfighters
- Rehearse TTP and Mission
- Range Assets Change Rapidly

Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

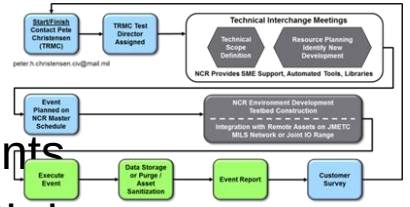
National Cyber Range Background, Vision and Mission

- **NCR Background**
  - Developed under DARPA in the 2009-2012 timeframe
  - Transitioned to TRMC in October 2012

- **Vision**
  - Be recognized as a premier cyberspace test range for providing mission tailored, hi-fidelity cyber environments that enable independent and objective testing and evaluation of advanced cyberspace capabilities and training Cyber Mission Forces.

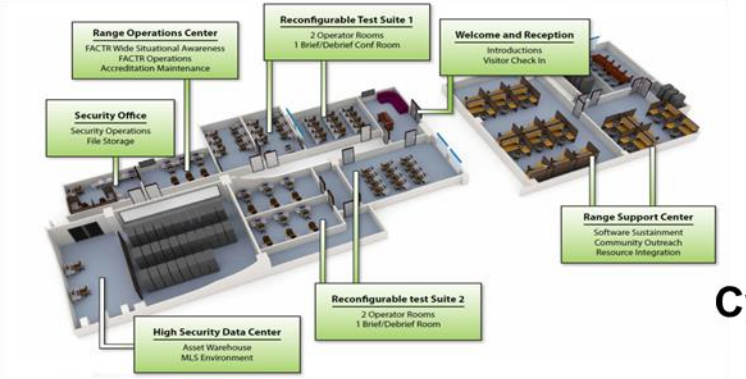


- **NCR Mission Statement**
  - Deliver Cybersecurity T&E and Training as a “Service” to meet customer requirements
  - Deliver secure facilities, innovative technologies, repeatable processes, and the skilled workforce
  - Deliver hi-fidelity, mission representative cyberspace environments
  - Integrate cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, DHS, industry, academia and international partners!

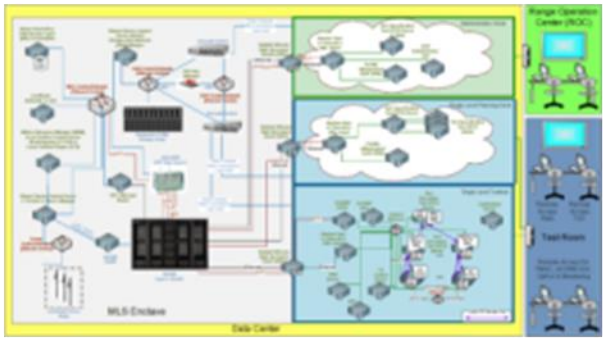


What is the National Cyber Range?

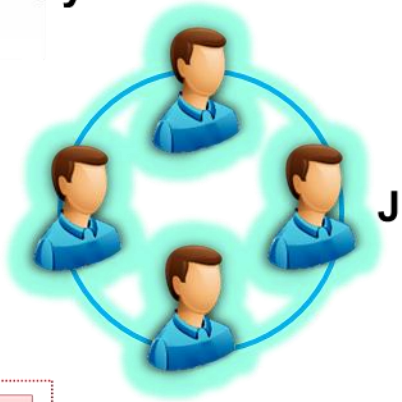
Computing Assets/Facility (LMCO Orlando, FL)



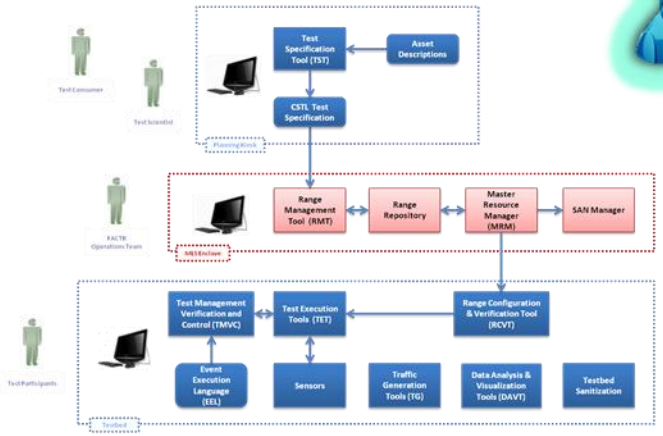
Encapsulation Architecture & Operational Procedures



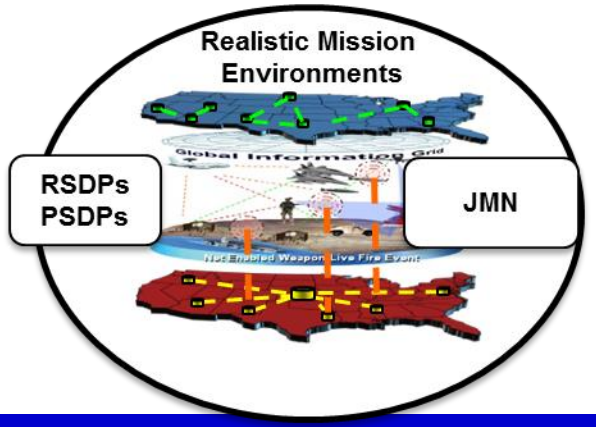
Cyber Test Team



Integrated Cyber Event Tool Suite



Secure Connectivity JIOR and JMETC MILS Network (JMN)



NCR is institutionally resourced by TRMC for DOD Customers!

NCR Unique Capabilities

- * Multiple Independent Levels of Security (MILS) architecture supports multiple independent tests beds at varying classification levels
  - DIA Accredited for testing up to Top Secret
- *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
- *Complex emulation of complex, operationally representative network environments
  - Can scale up to thousands virtual nodes
  - Red/Blue/Gray support, including specialized systems (e.g., weapon systems)
- *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 and communities
  - S&T, R&D, DT&E, OT&E, Controls Compliance, Vulnerability and Adversarial Assessments
  - CMF Training, IT Specialists, Incident Response Teams and Operators

*DARPA Hard Problems: MILS Architecture, Automation, Complex Emulation & Sanitization!

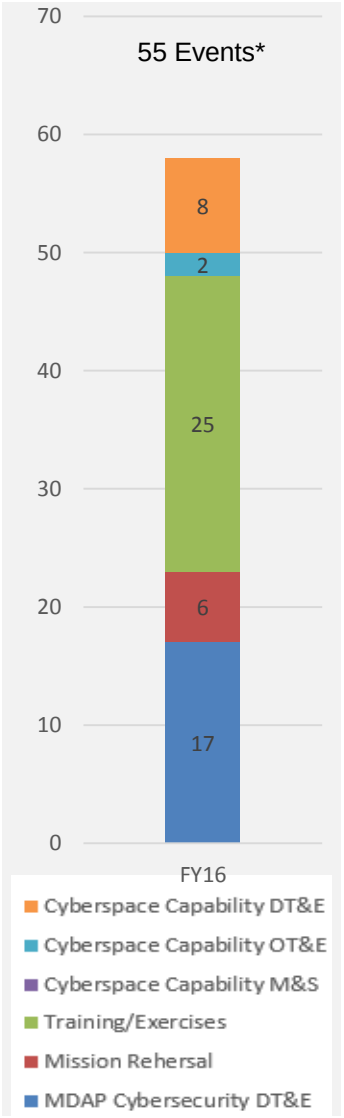
Five Reasons to Use a Cyber Range

- Lack of Resources creates “Test Data” Limitations:
  1. Unavailable to create a realistic Cyberspace/Cyber Threat Environments (security, fidelity, and/or scale)
  2. Unavailable to execute experimental designs to evaluate multiple controlled variables/scenarios

- Testing in an Operational Environment compromises Confidentiality, Integrity and/or Availability:
  3. Offensive/Defensive Cyberspace Operations expose sensitive vulnerabilities, tactics, techniques, procedures and/or capabilities employed by Cyber Mission Forces
  4. Testing causes unacceptable damage the System Under Test, connected systems or personnel
  5. Testing disrupts Military Operations, Operational Systems and/or Networks

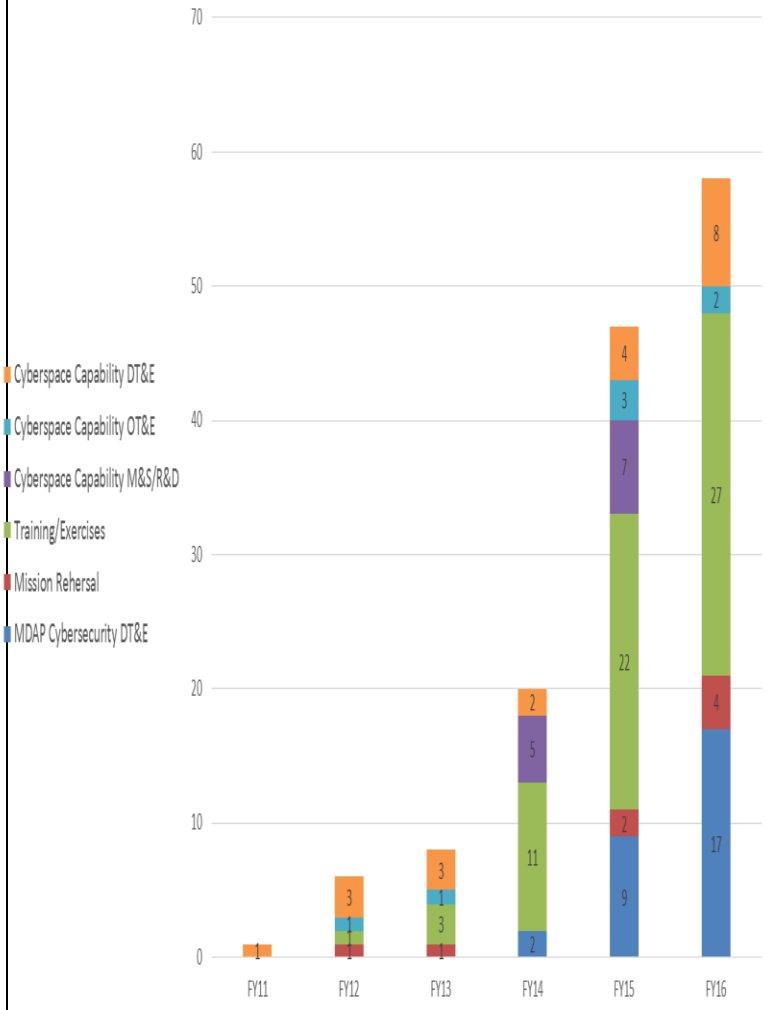
FY-17 Near Term
NCR Capacity Enhancements

- TRMC has worked to enhance capacity with all available computing resources including
  - Range Support Center (RSC)
  - NCR Classified Development Environment
  - Stand Alone Test Environment
  - 58 Events scheduled/executed in FY-16
- NCR conducted “Operational Pause ~15 Aug to 31 Oct
  - Periodic Security Re-Assessment and Authorization
  - HW and SW Recapitalization
  - ATO Awarded Feb 2017
- Capacity enhancements include adding
  - Doubled Test Beds
  - Five Fold Increase in Computing Assets
  - Tripled Storage Area Network Capacity



Cybersecurity Testing Lessons Learned

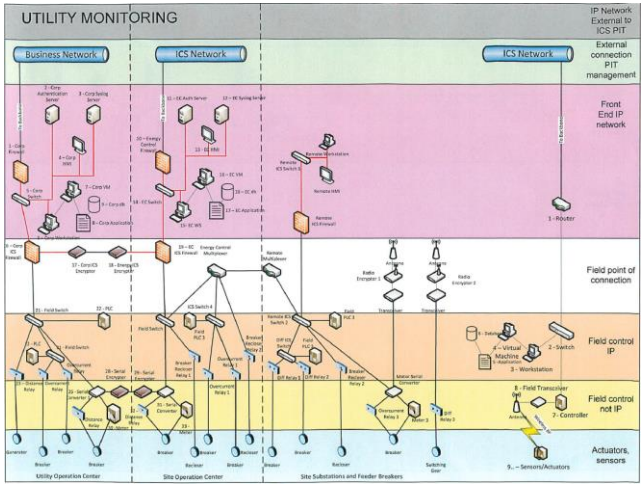
1. Start Small and grow
2. Testing is an important Engineering and Design Tool that can be used to refine requirements
3. Cyber Table Top is an effective tool to understand Mission Risks and prioritize testing
4. Focus Cybersecurity Testing on the Mission!
5. Cybersecurity Testing must be executed with key IT Staff, Incident Responders and Protection Teams
6. Customers need Cybersecurity T&E "As a Service"
7. Collaborative Approach to Coordinate Test Planning Critical
8. Effective Test Teams understand Cyber Offense and Defense
9. Automated Tool Suite creates efficiencies in event design, development and deployment
10. Connectivity makes range location irrelevant

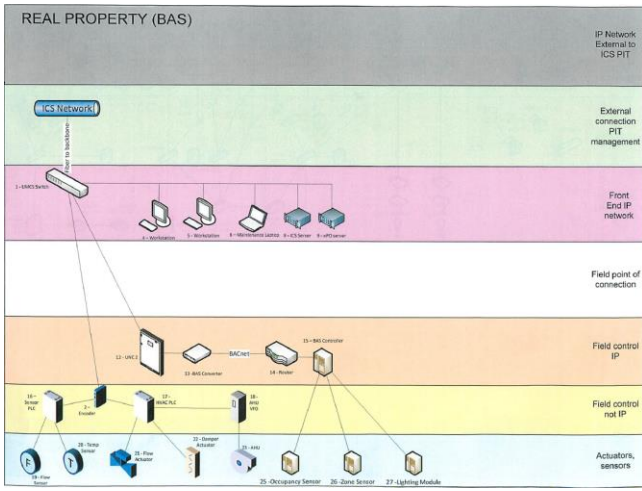


NCR Team executed 140 Events in 6 Years of Operation!

Pathfinder Event:
Control Systems Cyber Security (*CS²*) *Challenge*

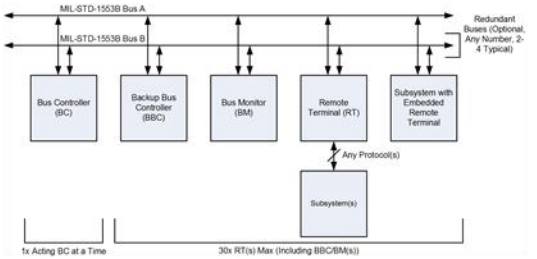
- Goal
  - Demonstrate DoD industrial and building control systems ability to detect, monitor, recover capabilities
- Relevance
  - Facility developers/managers have not considered Cybersecurity
  - Internet of Things makes Control Systems connected and exploitable
  - Commercially available protection systems and services typically have not been tested in real-world environments
- Next Steps
  - TRMC/NCR is collaborating with OASD Energy, Installations and Environment to build-out a complex/to-scale representation of a select, representative control system environment



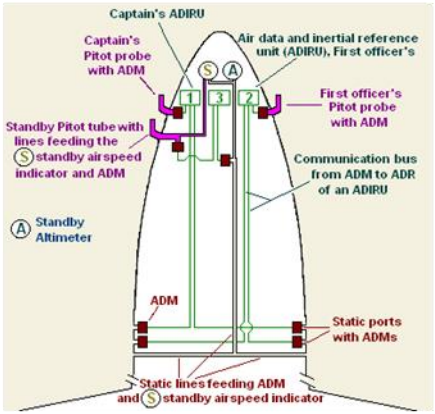


Pathfinder Event: Avionics Bus Architectures

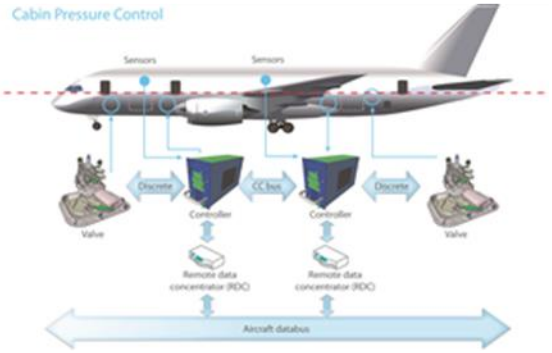
- Goal
  - Emulate Non IP Based Networks, Bus Architectures: MIL Std 1553, ARINC 429 for Cyberspace T&E



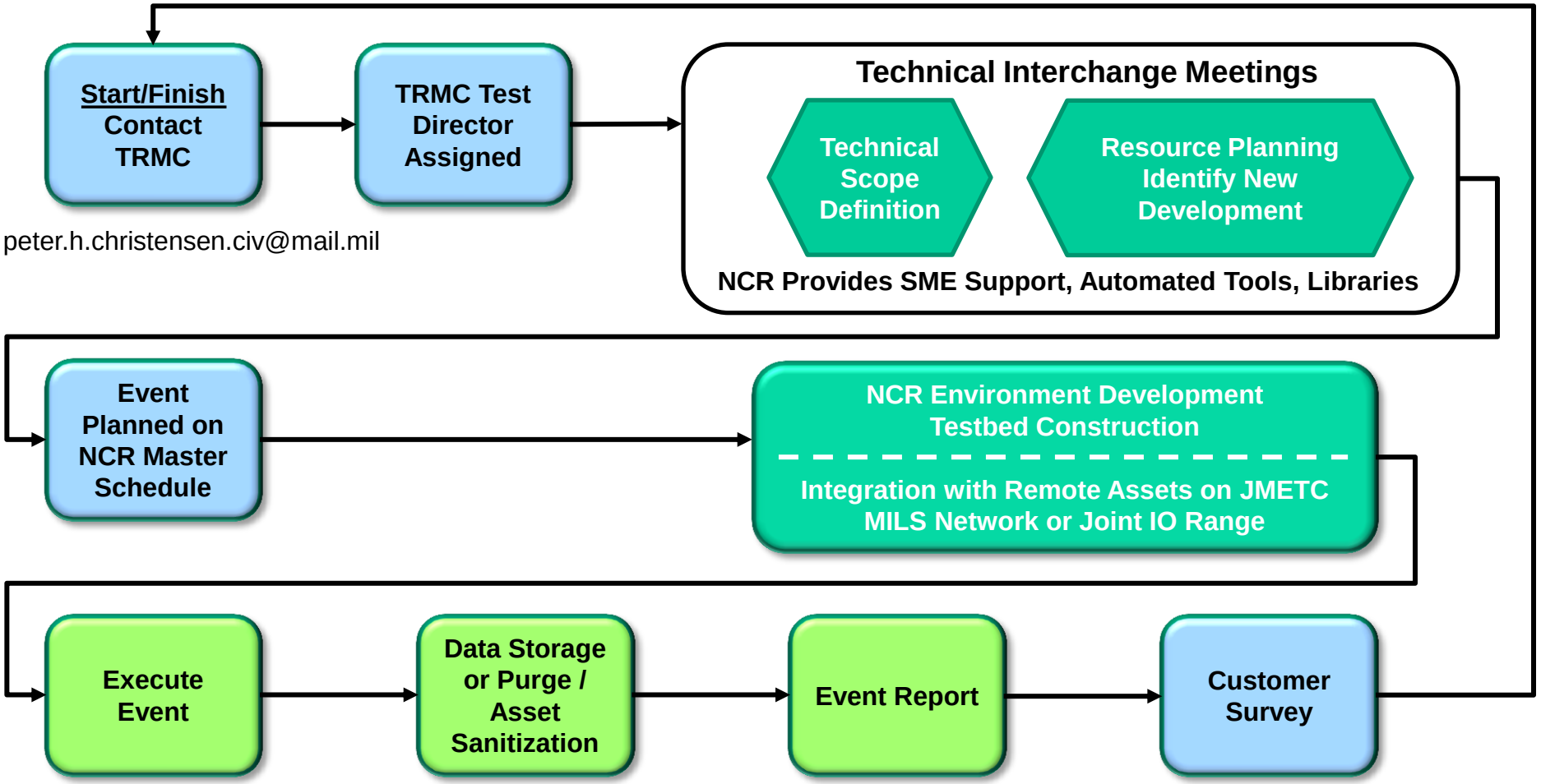
- Relevance
  - "Internet of Things" creates a massive Attack Surface
  - Cyber Threats demonstrated ability to exploit vulnerabilities in systems, subsystems and components
  - Some testing cannot/should not be conducted w/ actual aircraft, particularly in-flight



- Next Steps
  - TRMC/NCR collaborating with NAVAIR to build-out a complex representation of a typical Avionics Bus Environment
  - Range Events demonstrate and build upon capability
  - Verification and Validation essential



Process Flow for NCR Events



peter.h.christensen.civ@mail.mil

National Cyber Range Overview Day

- When : 15 March 2017
  9:00 AM to 2:30 PM
- Where: NCR in Orlando, FL
- What: An overview of the NCR will be presented including:
  - What type of testing you can do with the NCR
  - How to plan an NCR event
  - Example of Testing with the NCR
  - Example Training Event Environments Produced with the NCR
- Who: Government (or SETA) personnel who are interested in using the NCR
- Requirements: Minimum of SECRET Clearance
- Contact: Meredith Brehm
  meredith.brehm@lmco.com
  for more information about attending

Summary

- TRMC provides Cybersecurity Testing and Training as a service!
  - Over 140 Events executed in the first 6 years of operations
  - Supported a variety of events and customers
  - Developmental Testing, Operational Testing and Training/Exercises
- Rapidly evolving threat requires a new approach
  - Cyber Ranges provide agility needed to evolve with the adversary
  - Acquisition organizations can conduct system specific cybersecurity T&E tailored to meet program needs across the systems acquisition lifecycle
  - Operational organizations can conduct realistic cybersecurity training in environments that closely replicate the real world
- TRMC is enhancing existing capacity and capabilities
  - Demand continues to increase
- Lessons Learned are helping TRMC and NCR better support DOD
  - Pathfinders are leading the way!

Close Partnership Between Government and Industry Has Been a Critical Success Factor!

Questions?

Peter H. Christensen
Director, National Cyber Range
TRMC Office Phone: 571-372-2699
TRMC Email: peter.h.christensen.civ@mail.mil

Dr. Robert N. Tamburello
Deputy Director, National Cyber Range
TRMC Email: robert.n.tamburello.civ@mail.mil
Address:
4800 Mark Center Drive
Suite 07J22
Alexandria, Va. 22350

Cleared for Public Release
01 March 2017 Case # 17-S-1016