National Cyber Range

Distributed Testing with the NCR

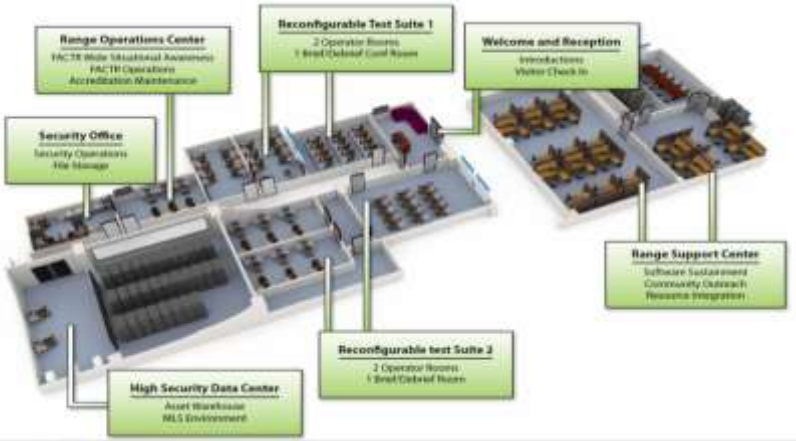
Lori Pridmore

National Cyber Range

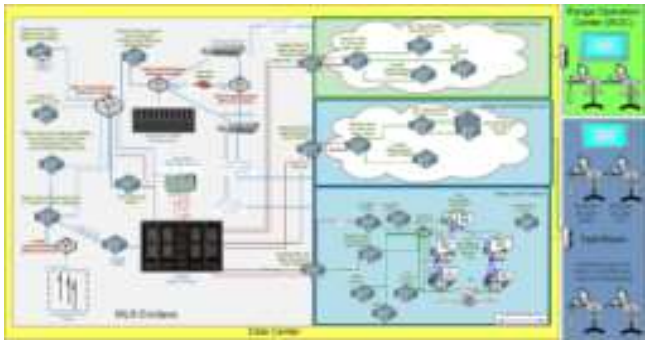
- Who are we?
  - National Cyber Range is a cyber testing and cyber training asset (facility, tools, trained staff) operated by Lockheed Martin for the Test Resource Management Center (TRMC)
  - The NCR facility is located in Orlando, Florida and is accessible remotely via the Joint IO Range (JMETC connection in process)

What is the NCR?

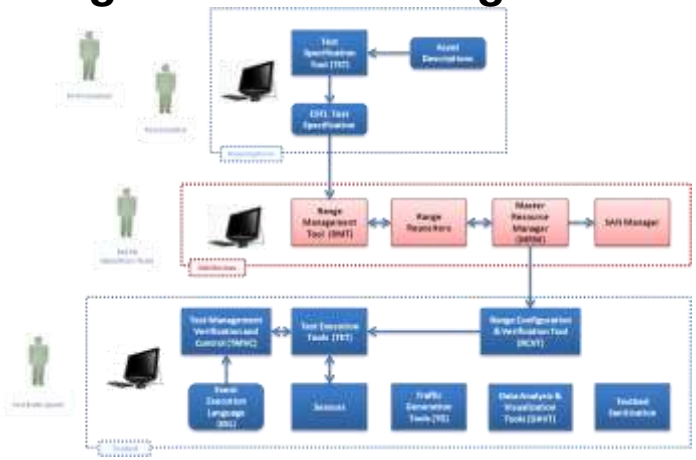
Computing Assets/Facility



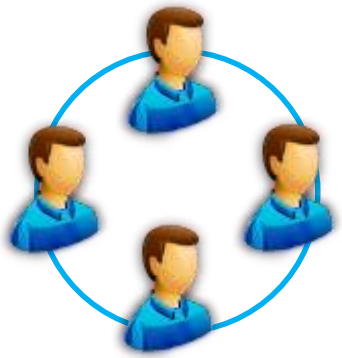
Encapsulation Architecture & Operational Procedures



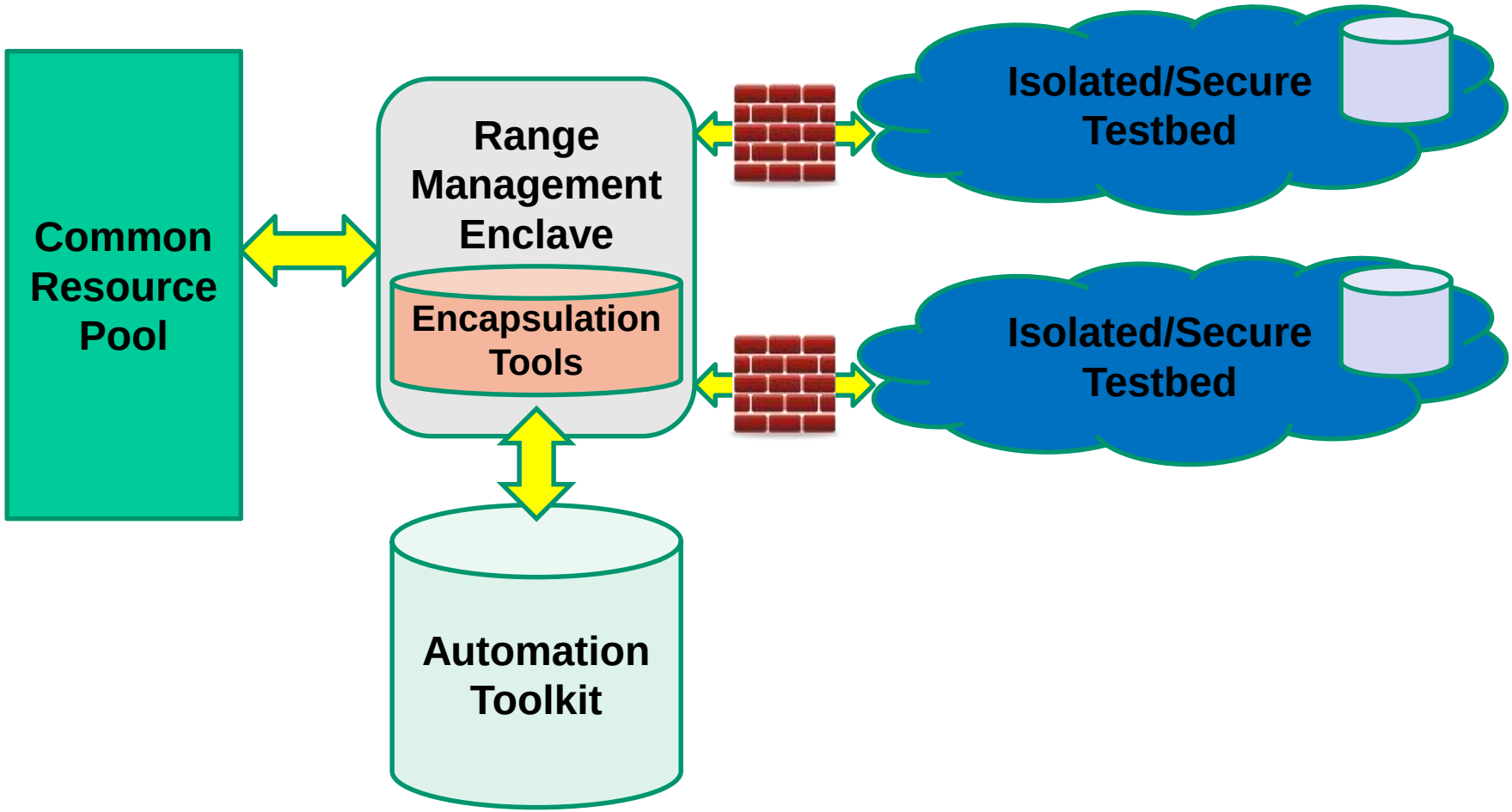
Integrated SW Testing Toolsuite



Cyber Test Team



Reconfigurable Range Concept

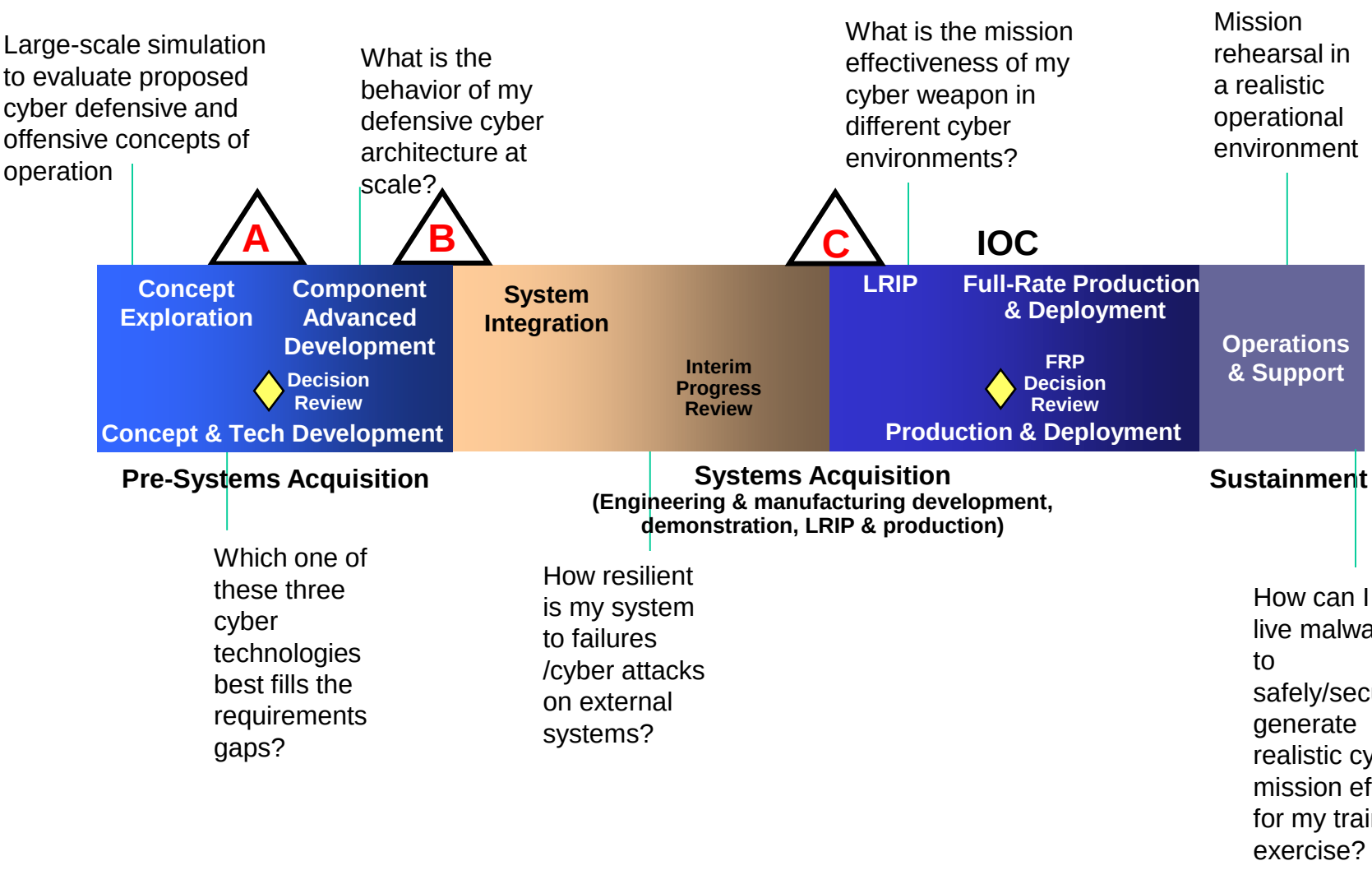


Partitions a common pool of resources into multiple independent testbeds

NCR Key Capabilities

- **Multiple concurrent tests at varying classification levels** are supported using a Multiple Independent Levels of Security (MILS) architecture
  - Currently support up to 4 events at varying classification concurrently
- **Rapid emulation** of complex, operationally representative network environments
  - Can scale up to ~50K 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.)

How Does NCR Fit Into the System Life Cycle?



Why Distributed Testing with NCR

- Provides a cyber testing environment to leverage from your site (without the investment of building and maintaining)
- Leverage the library of existing emulations and capabilities
  - Red/Gray/Blue Models
- Utilize live malware
- Enable remote red team
- Leverage large scale complex emulations
- Operate from your home base

Example 1 - Meridian

- **Use Case:** NCR provides the test environment and you run the test from your home location
- **Meridian:**
  - NCR Built and validated environment specified by the customer
  - Customer also did an independent verification
  - Customer loaded the system under test onto the environment
  - Customer conducted the test from their location
  - NCR packaged the resulting data and sent to the customer
  - Test Reconstitution

Remote Test Personnel

JIOR or JMETC

NCR provided test environment

Example 2 - Volley

- **Use Case:** Extend your own test environment and run at your home station
- **Volley:**
  - NCR provided diverse set of potential target platforms
  - Customer provided environment and System Under Test (SUT)
  - Customer conducted the test remotely
  - NCR provided traffic generation and instrumentation

Remote Test Personnel

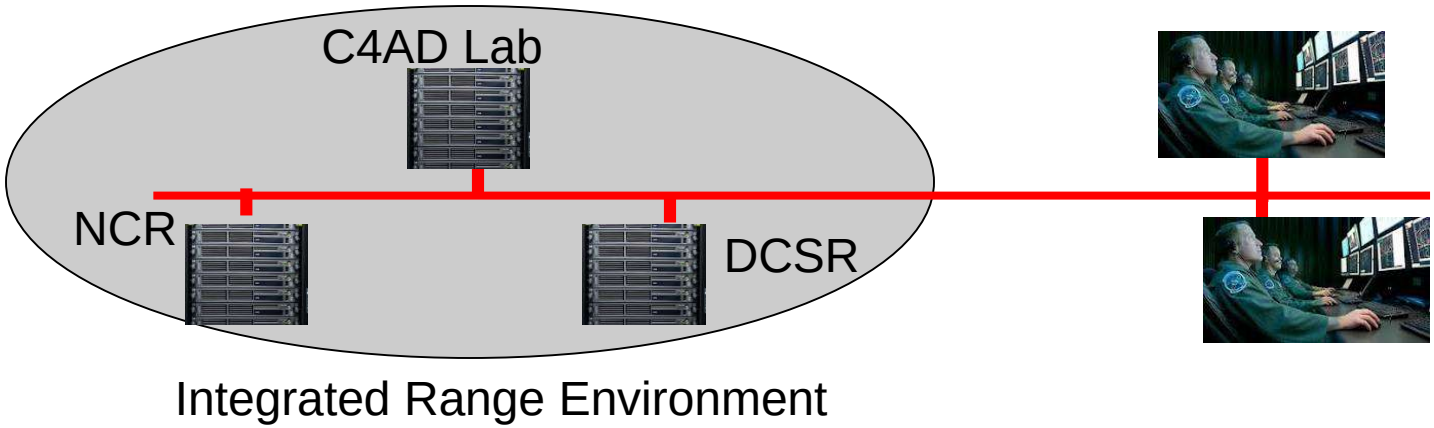
NCR provided test environment

Customer Provided test environment

JIOR or JMETC

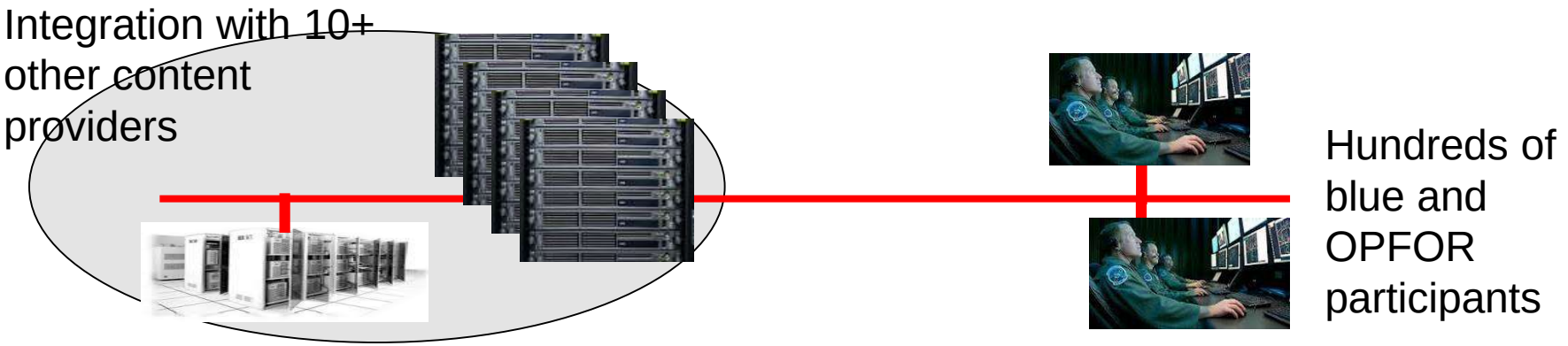
Example 3- ECRE

- Use Case : Enterprise Cyber Range Environment connecting live systems with emulation to produce a complex event environment
- ECRE:
  - Connected instantiations of production system (i.e. GCCS-M,…) with emulated environments
  - Remote red team
  - Remote test and training execution
  - Connection with other range



Example 4 – Cyber Flag

- **Use Case :** Complex Red (including OPFOR), blue and gray environment integrating kinetic assets
- **Cyber Flag NCR Content:**
  - Red network emulated environment
  - Shared gray emulated environment
  - Wireless network integration
  - Integration of kinetic assets
  - Over 40 logical ranges

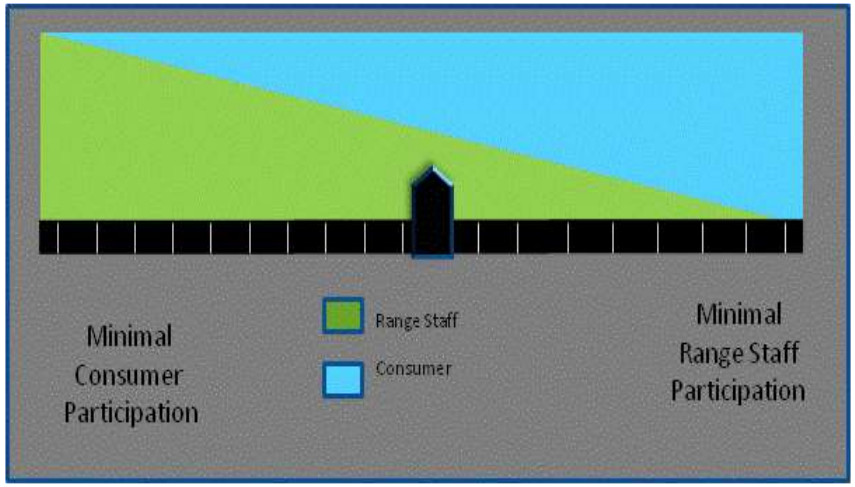


Large Scale Distributed Range Environment

NCR Services & Capabilities

- Technical planning for cyber test and training events
- Cyber SME support
- Red, blue, and gray space resources
- LVC assets
- Tools for automated event planning
- Data visualization
- Secure facility space for ~200 on-site event participants
- Repository of tools and assets
- Persistent training environments

- Simultaneous operation at multiple security levels
- Reach back to previous events
- Secure and partitioned test beds: complete isolation protects data and test results
- Sanitization of all assets

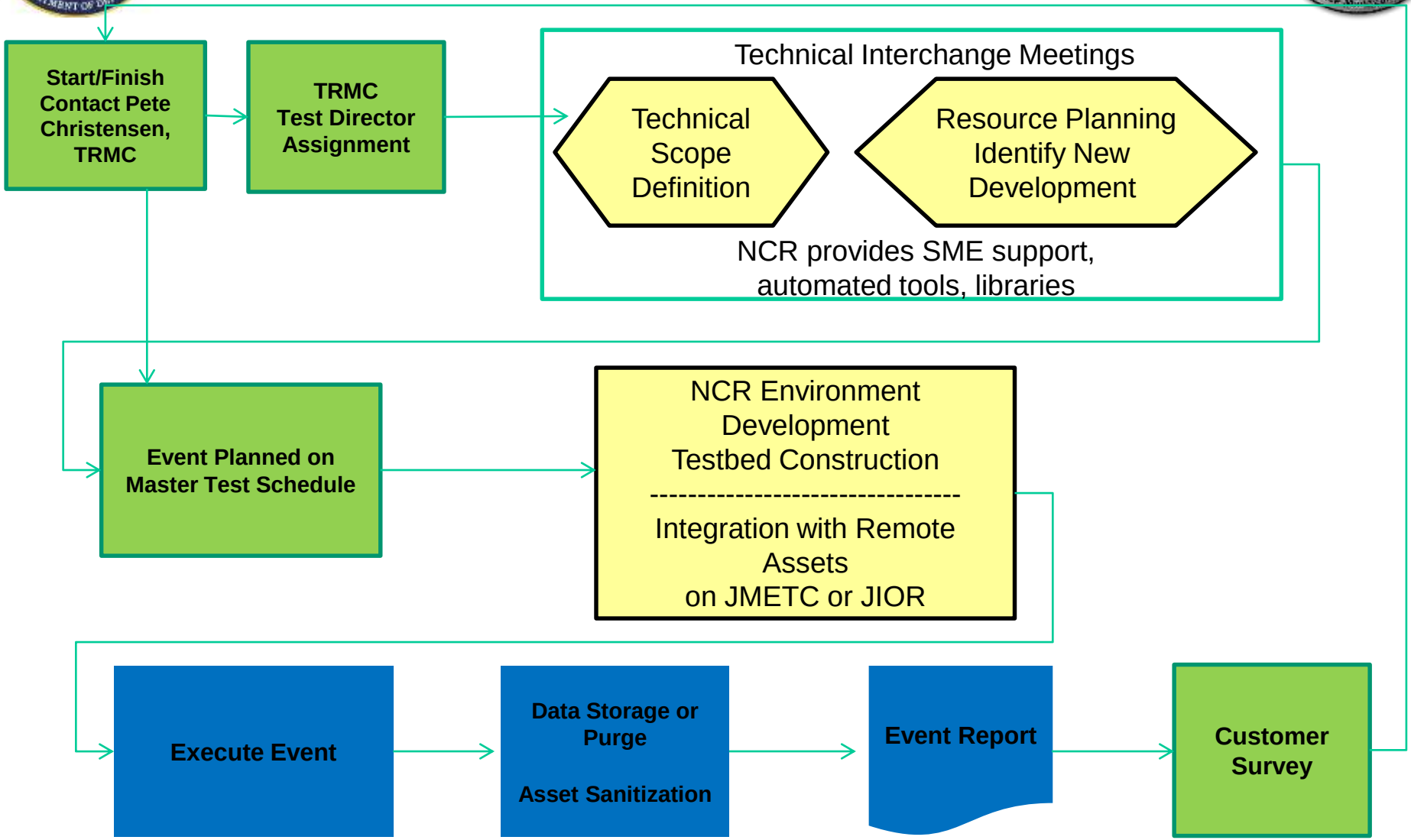


Services from range from providing a testbed to full end-to-end testing

2014 Range Schedule

July 88%	7-Jul	14-Jul	21-Jul	28-Jul	
	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	
	Triton	CYAMS	CYAMS	CYAMS	
August 100%	4-Aug	11-Aug	18-Aug	25-Aug	
	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	
	CYAMS	Cyber Flag 15-1	Cyber Flag 15-1	Cyber Flag 15-1	
September 100%	1-Sep	8-Sep	15-Sep	22-Sep	29-Sep
	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3	ECRE-C2IS-3
	Cyber Flag 15-1			Cyber Flag 15-1	Cyber Flag 15-1
October 100%	6-Oct	13-Oct	20-Oct	27-Oct	
	ECRE-C2IS-3	Vigilant Shield	Vigilant Shield	Vigilant Shield	
	Cyber Flag 15-1	Cyber Flag 15-1	Cyber Flag 15-1	Cyber Flag 15-1	
November 88%	3-Nov	10-Nov	17-Nov	24-Nov	
	Vigilant Shield	P-8A Placeholder	P-8A Placeholder	P-8A Placeholder	
			NSS	NSS	
	Cyber Flag 15-1	Sanitization	(Revised Date)		
December 75%	1-Dec	8-Dec	15-Dec	22-Dec	29-Dec
	P-8A Placeholder	Range Security Upgrades	Range Security Upgrades	Range Maintenance: Power & HVAC	
	NSS				

How To Use the NCR



For More Information…

- Pete Christensen - peter.h.christensen.civ@mail.mil
- Doug Troester – troester@mitre.org
- Lori Pridmore – lori.a.pridmore@lmco.com

Questions?