



The National Cyber Range



About NCR

The National Cyber Range (NCR), operated by the Test Resource Management Center (TRMC), provides the ability to conduct realistic cybersecurity testing, evaluation (T&E) and training. The four key components of the NCR are: a secure facility, a unique security architecture, integrated tools for cyber testing, and a multi-disciplinary staff. Accredited by the Defense Intelligence Agency (DIA), the NCR provides an efficient and affordable cybersecurity testing infrastructure that can operate at levels up to Top Secret / Sensitive Compartmented Information. Using state-of-the-art network isolation capabilities, the NCR can simultaneously execute up to four independent tests at different classification levels.

The NCR can represent complex network topologies with sufficient realism to portray a variety of current and anticipated attack strategies. The NCR's unique security architecture and sanitization tools enable the unconstrained use of malware during test and training events. In addition, the NCR's unique sanitization capability enables NCR provided test assets to be sanitized at the conclusion of an event and reused in future events at different classification levels. As a result, users can conduct advanced developmental and operational tests and evaluations, and provide realistic operational training in environments that emulate specific computing, networking, and information systems environments.

The NCR enables users to assess many different aspects of cyber capabilities throughout the development and operational lifecycle (Figure 2). Events can be executed locally using secure test rooms located at the NCR or remotely via the Joint Information Operations Range (JIOR), and the Joint Mission Environment Test Capability (JMETC) in the future. Users can also integrate their program or organization unique cyber assets into an NCR environment as "black boxes" that become an integral part of the environment without the need for range security reaccreditation.

The NCR has demonstrated the ability to rapidly configure a variety of complex network topologies and scale up to 40,000 nodes. These nodes can include high-fidelity realistic representations of the public internet infrastructure including highly detailed supporting web and email servers and clients. The ability of the NCR to emulate sensitive DoD network enclaves adds a high degree of realism and value to events.

The world-class multi-disciplinary staff that operates the NCR enables DOD, Intelligence Community, and other government organizations to design and conduct effective, and cost efficient cybersecurity T&E and training events. Experts in offensive and defensive cybersecurity, testing, and software development skills can engage with users to address a wide variety of complex cybersecurity challenges.

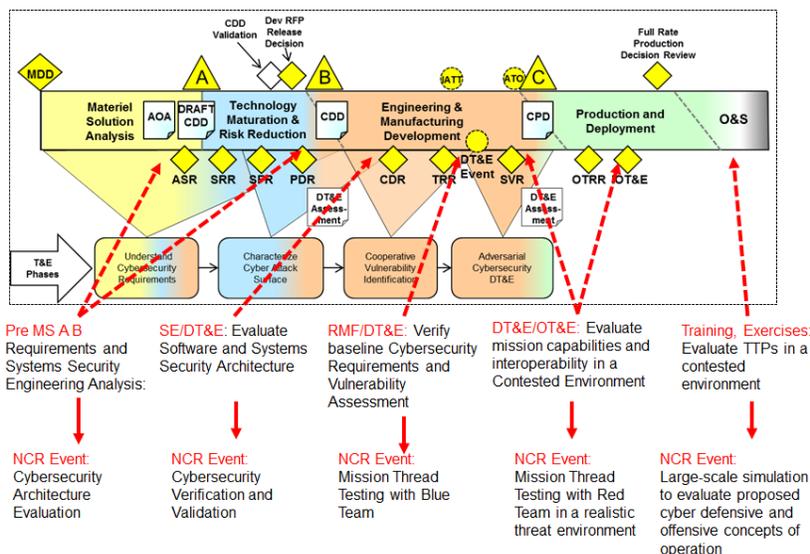


Figure 2. NCR Lifecycle Support

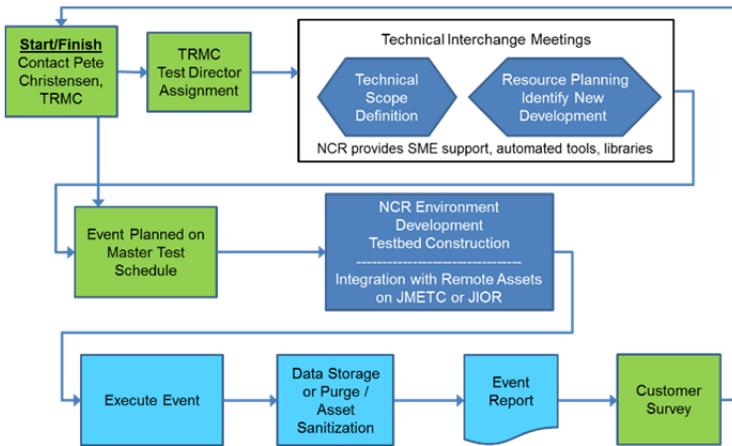
Benefits of Using the NCR

By leveraging NCR resources, government organizations have gained valuable insights into how well their existing information technologies can meet the demands of a rapidly evolving cybersecurity landscape. With a highly scalable, secure, and extremely flexible range capability, expensive questions can be answered quickly, accurately, and safely. This can be achieved at a fraction of the cost associated with building and operating a similar customer-owned capability.

The NCR can help assess how resilient a system is to cybersecurity-attacks and faults as an independent system or when connected to a larger system-of-systems architecture by augmenting the existing operational environments. If a program wanted to evaluate the effectiveness of its cyber offensive and defensive capabilities, it can exercise and experiment with those capabilities at the NCR – with no adverse impacts to the program-owned infrastructure.

Additional Features of the NCR include:

- **Customer-Driven Test Specification:** Allows NCR customers to specify the testbed configuration.
- **Wireless Testing Support:** Wireless assets can be incorporated into a testbed through use of the on-site Faraday Cage.
- **Supported Software:** The NCR supports most major operating systems and a wide compliment of supporting infrastructure tools from routers and switches to web servers, firewalls, and intrusion detection systems. If not already available at the NCR, the NCR has an efficient processes for incorporating additional software to a testbed.



NCR Event Workflow

Figure 3. NCR Event Workflow

The first step to arranging an NCR event is to contact a TRMC NCR representative (Figure 3 and email provided below). The NCR team will work with users to shape the technical scope of their event, allocate resources and identify any required custom integration through a series of technical interchange meetings between NCR Test Directors, technical subject matter experts, and user representatives. Once the scope of the event has been defined, the event is scheduled for range time.

Prior to execution, the NCR staff will use the test specification that is the product of the technical interchange meetings and “build out” the testbed. The build process includes the partitioning of the testbed, allocating system resources to the test, and integration and configuration of additional assets that are part of the test specification. Once the build process is complete, the testbed is ready to go “range hot” – and is prepared for the event to start.

During the event, customer-specified data can be collected through the NCR’s suite of data sensors and visualization tools. Data that is collected during an event belongs to the customer and will be released or shared without first receiving the customer’s approval.

Once an event has concluded, a test report is generated and all assets used during the event are sanitized—leaving no trace of an event’s testbed or the data.

Cyber Policies

The following policy documents provide acquisition guidance to Program Managers and T&E practitioners through developmental and operational test activities.

- **Revision of DoDI 5000.02: Issued 6 Jan 2015**
 - New/better guidance for both developmental and operational testing of IT
 - <http://www.acq.osd.mil/fo/docs/500002p.pdf>
- **Revision of DoD 8500.01, Cybersecurity: 14 Mar 2014**
 - Expanded scope and specificity
 - <http://www.dtic.mil/whs/directives/corres/pdf/8500012014.pdf>
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: 14 Mar 2014**
 - Provides policy, clarity and guidance on the RMF and compliance
 - <http://www.dtic.mil/whs/directives/corres/pdf/8510012014.pdf>
- **Four Phased Cybersecurity DT&E Process: In Work**
 - Incorporated into Defense Acquisition Guidebook Chapter 9
 - <https://acc.dau.mil/CommunityBrowser.aspx?id=504118>
- **OSD DOT&E- Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: 01 Aug 2014**
 - Formalizes OT&E Phases
 - [http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs\(7994\).pdf](http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf)
- **Cybersecurity Implementation Guidebook for PMs**
 - Address Cybersecurity T&E across the acquisition lifecycle
 - Not available yet
- **Cybersecurity T&E Guidebook planned**
 - To provide detailed Cybersecurity T&E guidance for DT/OT Community
 - Not available yet

For More information email NCR:

osd.pentagon.ousd-atl.mbx.trmc-ncr@mail.mil