Cyber Security Range

Enabling Dominance in Cyberspace

James Curry, Lead Engineer
DISA ID25, DoD Cyber Security Range
26 March 2019
What is the DoD Cyber Security Range?

Test, Train, Exercise, Evaluate

The mission of the Cyber Security Range (CSR) is to provide a representative network environment to the current cyberspace domain to allow realistic Testing, Training and Evaluation of cyber warriors and their cyber related tools.

Realistic IT Network Models

- Various ranges of fidelity
- Rapidly Provisioned
- Remotely or Locally Accessible

End State: DoD’s Information Network’s security posture is strengthened and the ability to Protect and Defend DoD networks is increased.
DoD CSR Niche Capabilities

- Virtual Joint Regional Service Stack: vJRSS
- Virtual Internet Access Point: vIAP
vJRSS

- JRSS is a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding (VRF), and provides a host of network security capabilities
- vJRSS is a mirror of the JRSS pre-production stack, built entirely from virtual technology
- Identical capabilities for active routing, passive analysis, and JMN management
- All B/P/C/S traffic traverses vJRSS (e.g. Inter-VLAN, Inter-Base, Inter-Agency, Internet)
- Currently used for CPT exercises and CND scenario training
- Future state includes NetOPs scenario training

**Note:** Current licensing can support a full stack of capabilities; 1 classification level at a time and 1 event at a time.
• Tier 1 Service that provides the first line of defense between the Internet and the DoDIN

• Suite of capabilities that provide:
  • Web Content Filtering (WCF): Palo Alto, Splunk, ArcSight
  • Enterprise Collaborative Operational Sensors (ECOS): (SourceFire, SiLK, WireShark, Bivio)
  • Distributed Denial of Service Threat Reduction (DDoS-TR): Arbor

• Realistic routing between Virtual Internet and Tiers 2 & 3
• Piloting in DISA Defender 18

Note: Current licensing can support a full stack of capabilities; 1 classification level at a time and 1 event at a time.
# Core Capabilities

<table>
<thead>
<tr>
<th>Core Capabilities</th>
<th>UNCLASS CTEP Access</th>
<th>UNCLASS VPN/DBS Access</th>
<th>SECRET JIOR Access</th>
<th>TS/SCI JIOR Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Internet</strong></td>
<td>Social Networks</td>
<td>Juniper Routing</td>
<td>Core NIPR routing</td>
<td>Unclass Enclaves</td>
</tr>
<tr>
<td></td>
<td>E-Commerce sites</td>
<td>ECOS</td>
<td>Border Gateway Protocol</td>
<td>Classified Enclaves</td>
</tr>
<tr>
<td></td>
<td>Domain Name Services</td>
<td>DDOS Protection</td>
<td>Border Gateway Protocol</td>
<td>Active Directory</td>
</tr>
<tr>
<td></td>
<td>Network Time Protocol</td>
<td>Web Content Filtering</td>
<td>Border Gateway Protocol</td>
<td>Exchange Email</td>
</tr>
<tr>
<td><strong>Exercise Control</strong></td>
<td>User Emulation (LARIAT)</td>
<td>Mission Impact</td>
<td>Administration of users, roles, networks, events</td>
<td>Tracker for Red and Blue action</td>
</tr>
<tr>
<td></td>
<td>0-Day Emulation &amp; Auto-OPFOR</td>
<td>0-Day Emulation &amp; Auto-OPFOR</td>
<td>0-Day Emulation &amp; Auto-OPFOR</td>
<td>Attack Visualization</td>
</tr>
<tr>
<td></td>
<td>Network Monitoring &amp; Replay</td>
<td>Network Monitoring &amp; Replay</td>
<td>Network Monitoring &amp; Replay</td>
<td></td>
</tr>
<tr>
<td><strong>Automation</strong></td>
<td>Resource Provisioning</td>
<td>Workflow Orchestration</td>
<td>SIMSTIM</td>
<td></td>
</tr>
<tr>
<td><strong>Transport</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Core Capabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSR Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B/C/P/S</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NetOps Capabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>JMS Functionality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Traffic Generation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UNCLASSIFIED**

**Trust in DISA: Mission First, People Always!**
The Future of the CSR

- **Additional DoDIN Enterprise Capabilities**
  - Enterprise Email (EEMSG)
  - PKI & Certificate Management
  - SSL Break and Inspect
  - Big Data Analytics and Machine Learning

- **Additional CSR Capabilities**
  - Improved environment accessibility for remote configuration management
  - PCTE Support and Integration
Points of Contact

Cyber Range Management Team:  
MCCR Program Manager:  
Office: (703)445-3847

MCCR@usmc.mil

DoD CSR Program Manager:  
Office: (301)225-4561

DoDCSR@mail.mil

703-445-3650
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil /USDISA @USDISA