DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

CyberSecurity Range (CSR) v2.0 Architecture and Capability

James Curry
Lead Engineer, DoD CyberSecurity Range
22 April 2016

Presentation Disclaimer

DISA

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."
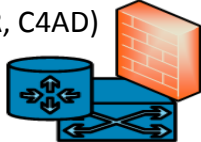
DoD CyberSecurity Range (CSR) 2.0 Agenda

DISA

- Background
- BLUF
- CSR v2.0 Design
- Target States for FY 17 & 18
- Use Case – JRSS Virtual Training Environment
- CSR v2.0 Demo

DoD CyberSecurity Range v1.0 Background

- Form replication of DoDIN in multiple classifications
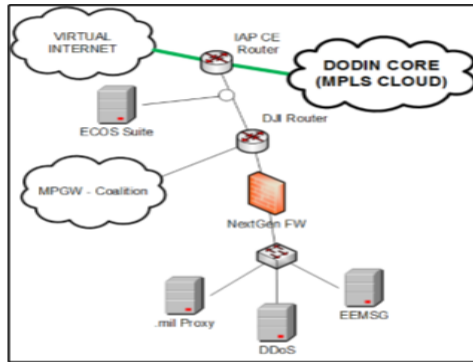- Supports Exercises, Training, and Testing
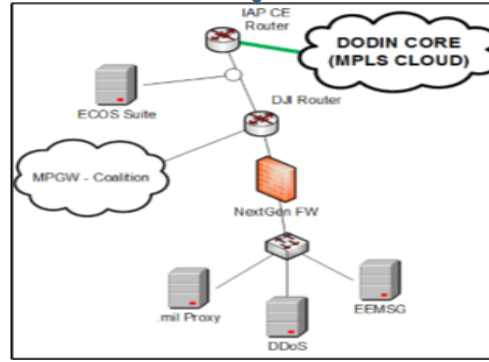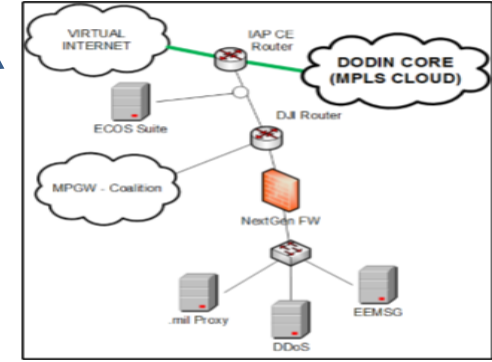

Federated DECRE Ranges
(JIOR, NCR, C4AD)

Zone C

UNCLASSIFIED VTE

UNCLASSIFIED CSR

SECRET CSR

TS/SCI CSR

DoD CyberSecurity Range (CSR) BLUF

DoD CSR Issues

- Labor-Intensive Manual Event Configuration
  - Little time spent on topology validation.
  - Topology validation usually occurs "in-event" & detracts from event goals.
- Nonaligned Range Infrastructure Segments
  - Many Event Capabilities Require Coordination Across All Segments.
- Range Scheduling & Growth Impacted by new demand signal
  - Conflict on computing resources/hardware/software.

Way Ahead

- Common Range Automation Framework at all levels of classification.
- Automated environment control & provisioning.
- Integrated & automated commodity HW, virtualization, & specialty HW control.

DoD CSR v2.0 Next Gen Design

Approach

Common resource object definition for CSR virtualization, specialty HW, & commodity HW resources

| Resource Authoring | ◆ | Event Authoring | ◆ | Event Orchestration | ◆ |

Benefits

- Persistent pool of resource objects enabling subsequent event authoring consistency

- Automation objects enabling subsequent event authoring & orchestration efficiencies

- Automation objects provide configuration, validation, monitoring, control, & assessment capabilities

DoD CSR v2.0 Next Gen Design

Approach

Graphical drag-n-drop topology configuration from persistent library of resource objects

| Resource Authoring | ◆ | Event Authoring | ◆ | Event Orchestration | ◆ |

Benefits

- Automated event topology definition

- Event topology built from unified view of all CSR resources – virtual, specialty HW, & commodity HW

- Automation linked to event topology for event-specific configuration, validation, monitoring, control, & assessment

DoD CSR v2.0 Next Gen Design

Approach

Single point of automated orchestration for all CSR virtual, specialty HW, & commodity HW resources

| Resource Authoring | ◆ | Event Authoring | ◆ | Event Orchestration | ◆ |

Benefits

- Automated event topology instantiation

- Automated instantiated event topology validation

- Automated in-event resource usage metrics & response
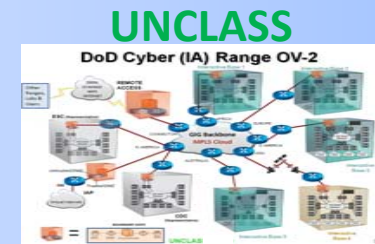
- Automated in-event control & assessment

DoD CSR v2.0 Target State FY17 – FY18

DoD CSR DoDIN/DISN

- **Tier 1**
  - **DISN Core Router Backbone**
  - **DODIN DNS Core Service**
  - **MPLS Routing**
  - **Sensing Nodes**
  - **Internet Access Points (IAP)**
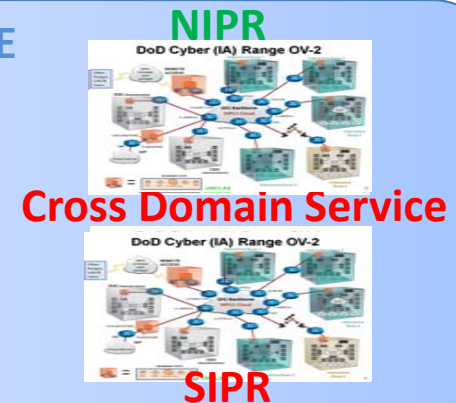 - **Joint Regional Security Stack (JRSS)**

DoD CSR 2.0 UNCLASS RANGE

- UNCLASS Tier I
- Leveraging DISA IAP and JRSS All other components down at the CSR

UNCLASS

DoD CSR 2.0 CLASSIFIED RANGE

- Full Hybrid (Virtual/Physical) Tier I at the NIPR and SIPR networks
- Full Virtual Infrastructure IAP and JRSS Stack at DoD CSR
- CDS between Networks

NIPR

Cross Domain Service

SIPR

# What CSR v2.0 brings to Cyber Range space

DoD CSR 1.0

- Major Physical Equipment
- Physical Rack and Stack
- Labor intensive configuration

DoD CSR 2.0

- Virtualize physical equipment to the greatest degree possible
- Manage Virtual infrastructure over browser technology
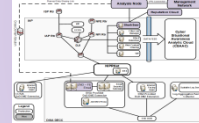- Build Gold level infrastructure environment to used repeatable in training and exercises
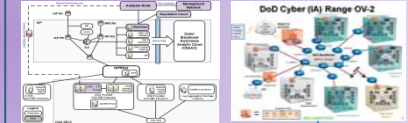

DoD Cyber (IA) Range OV-2
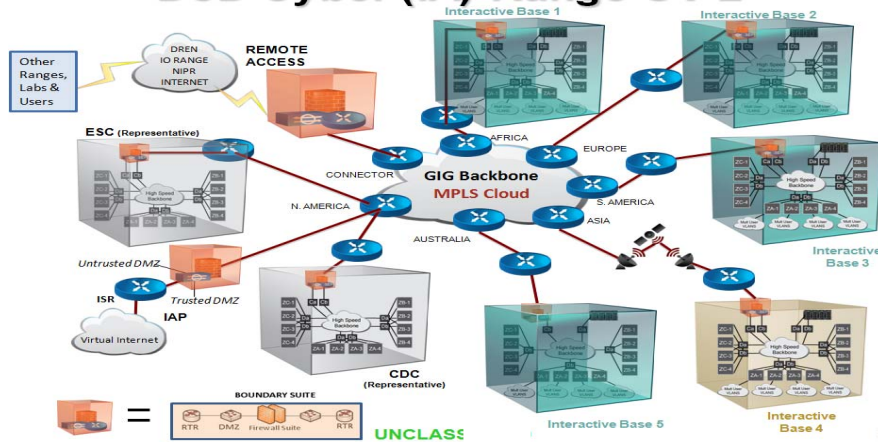
Physical Infrastructure
Blue Coat SSL Decryptor

Virtual Infrastructure
IAP Container   DISN Core Container
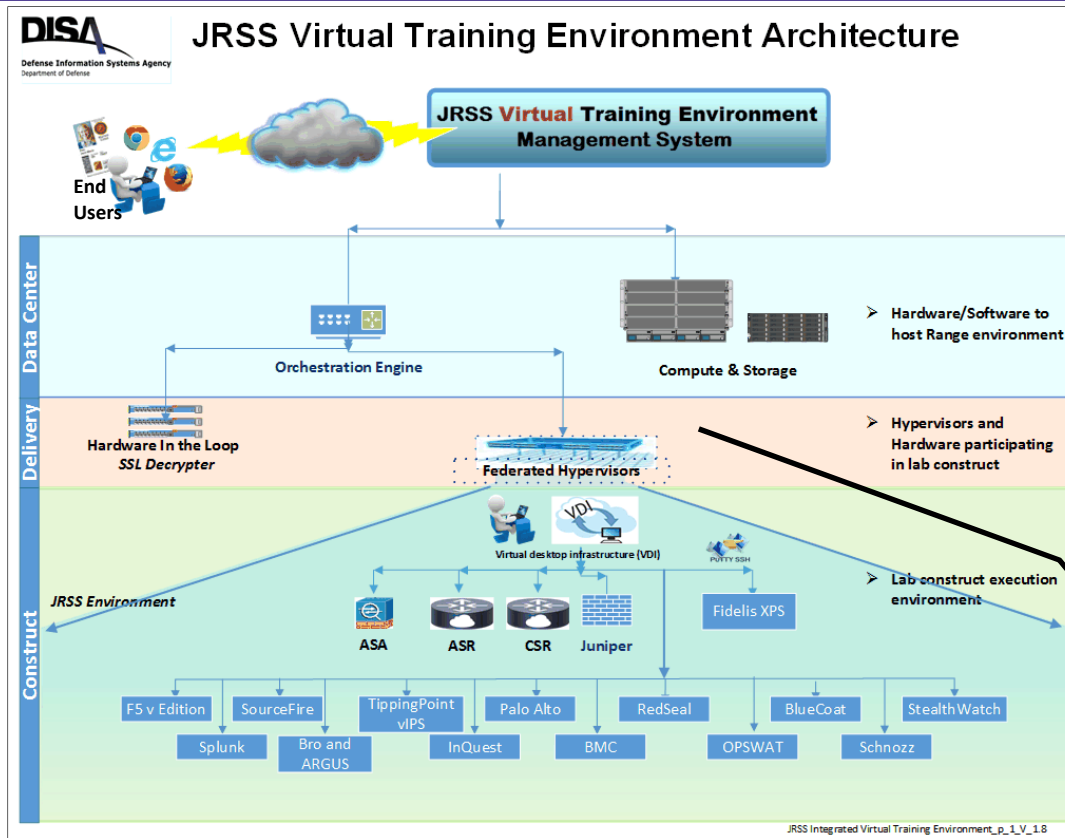
Use Case 1
- Teach via Distant Learning Mechanism
- Use training event in the JRSS VTE for TTP or Lab guide execution

Use Case 2
- Teach in traditional classroom.
- Use training event in the JRSS VTE for TTP or Lab guide execution

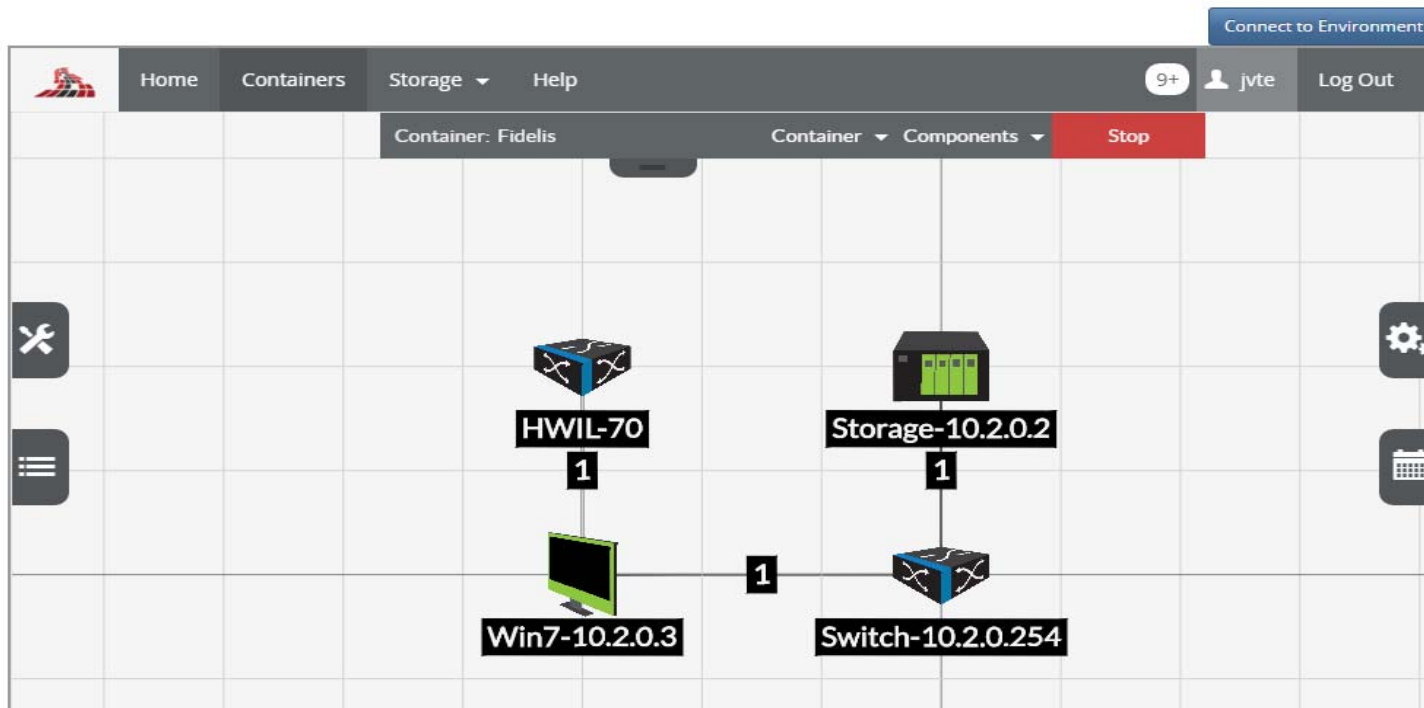JRSS Virtual Training Environment Architecture

Benefits
- Reduction in TDY Cost.
- Bring your own certified device.
- Train in a operational virtual infrastructure container.

Virtual JRSS Infrastructure

Fidelis Training environment with JVTE

CSR Contact Info

- **CSR Customer Management Team
  CRMT@mantech.com**

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION