DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

AFCEA DISA CyberNetOps (CNO) Solutions

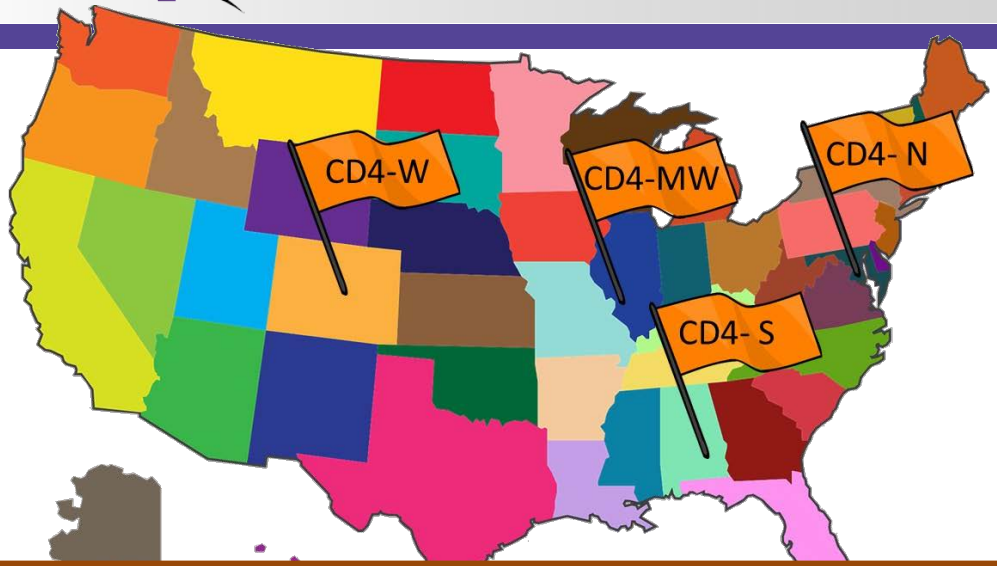
James Travis, PhD, CEH

Cyber SA/NetOps Directorate
14 June 17

V5.1

CD4 Mission

Who We Are



CD4, a Cyber Directorate Division, provides Operational Support System Solutions for DISA's command and control and information-sharing capabilities to DISA Operations & DISA's Mission Partners

FOCUS

- Assuring DoDIN operations (transport, compute, apps)
- Optimize capabilities to enable software defined networking (SDN) and network function virtualization (NFV)
- CyberNetOps tools convergence
- Adopt open source and white box solutions
- CyberNetOps via moble applications

ID4 CyberNetOps Leadership

Who We Are

Robert Mauldin
Chief, NetOps PMO/Architecture Integration
(ID41)

CyberNetOps Division

James Travis, Division Chief

Alfrenetta Cooper, Deputy
Vacant, Chief Engineer

Thomas Hines
Chief, Network/Service Management Systems (ID43)

Scott King
Chief Engineer (Acting)
Chief, Network Element Systems
(ID42)

Andrew Cape
Chief, Computing Management Systems (ID44)

CyberNetOps (OV-1)

What's the Operating Environment

Service Desk

DISA Workers

Mission Partners

Command & Control

Service Managers & PMs

Operations & DCO

DoD Senior Leaders

Display Layer

Workflow Transactions

Alerts & Alarms

Knowledge Management (KM), Business Intel (BI) & Analytics Queries

Workflow Data

ITSM

Request/ Requirement & Demand

Change & Config

Design & Build

Capacity , Availability & Continuity

Event, Incident & problem

Knowledge Centered Support

Service Level Management

Access, Security and CNDSP

Workflow Tools

BI/KM/Analytics Engines

Data Element & Artifact Associations

NIPR Data Warehouse

Cross Domain

SIPR Data Warehouse

Data Warehousing

Data Tagging Strategy

Translation Layer

Logs

EMS

PerfMS

CM

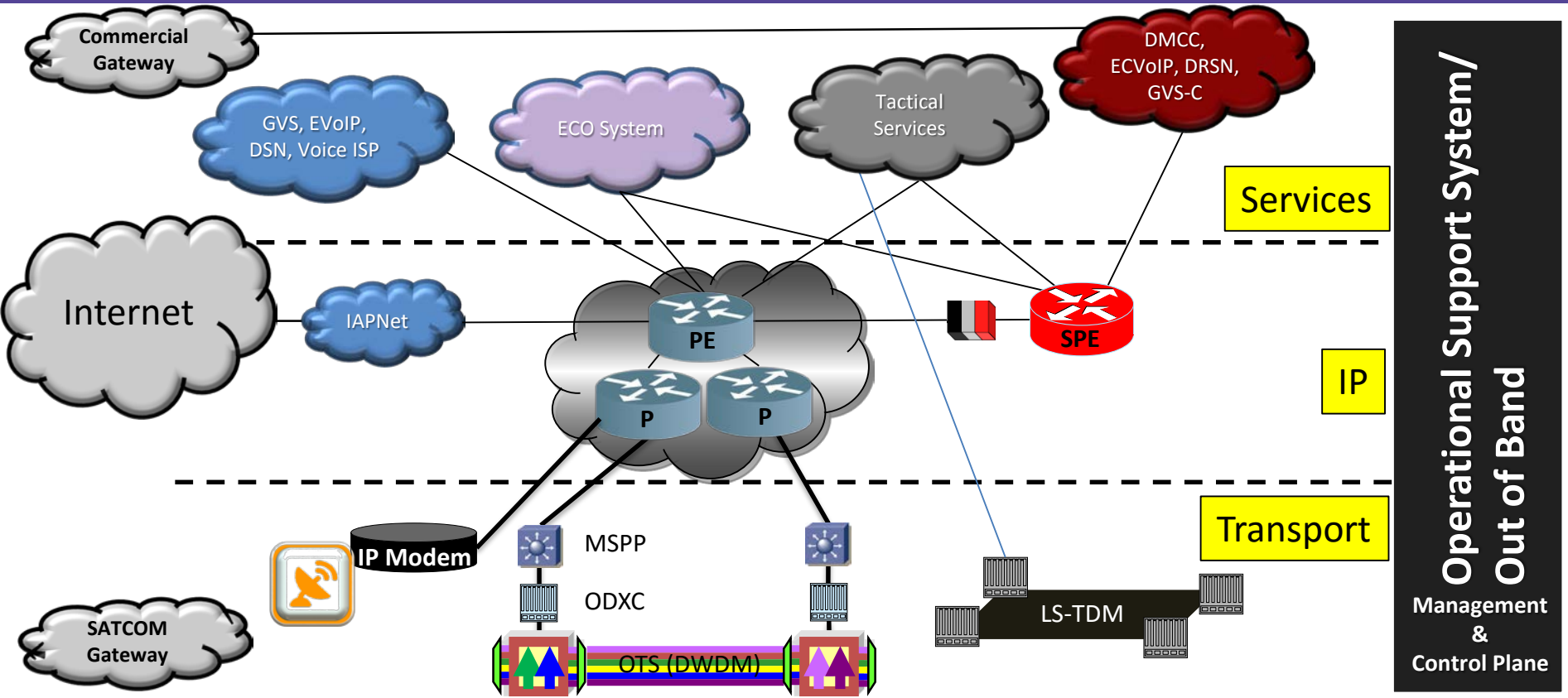
DODIN Security

CYBEROPS

The Data Layer

DODIN Operations Mission Areas (SV1)

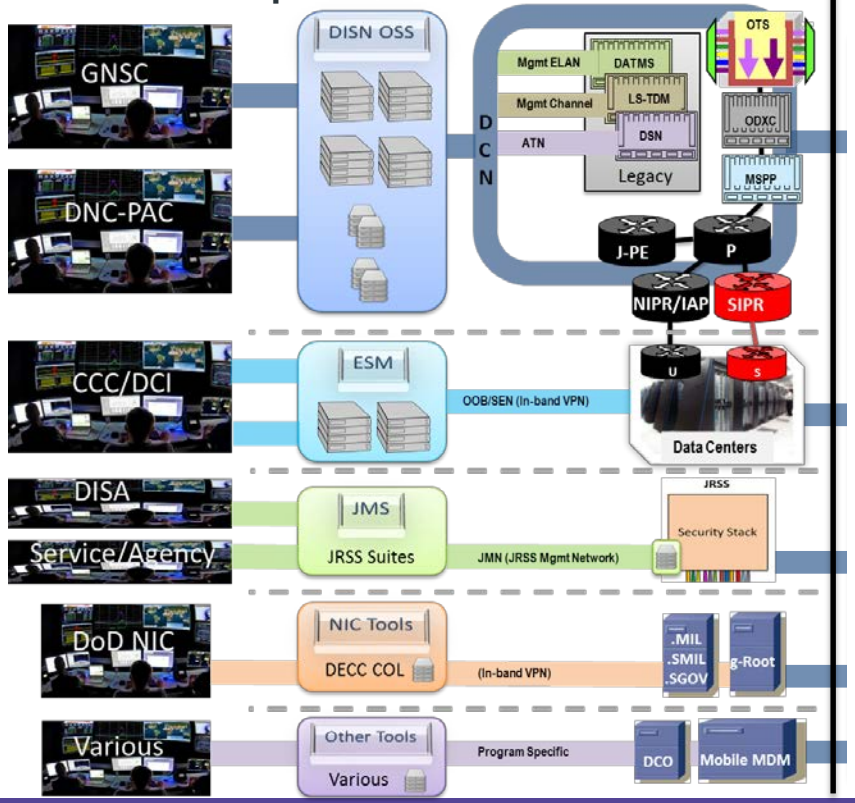
What's the System Env



DISA Telemetry & Control - Future

What's the Telemetry Env

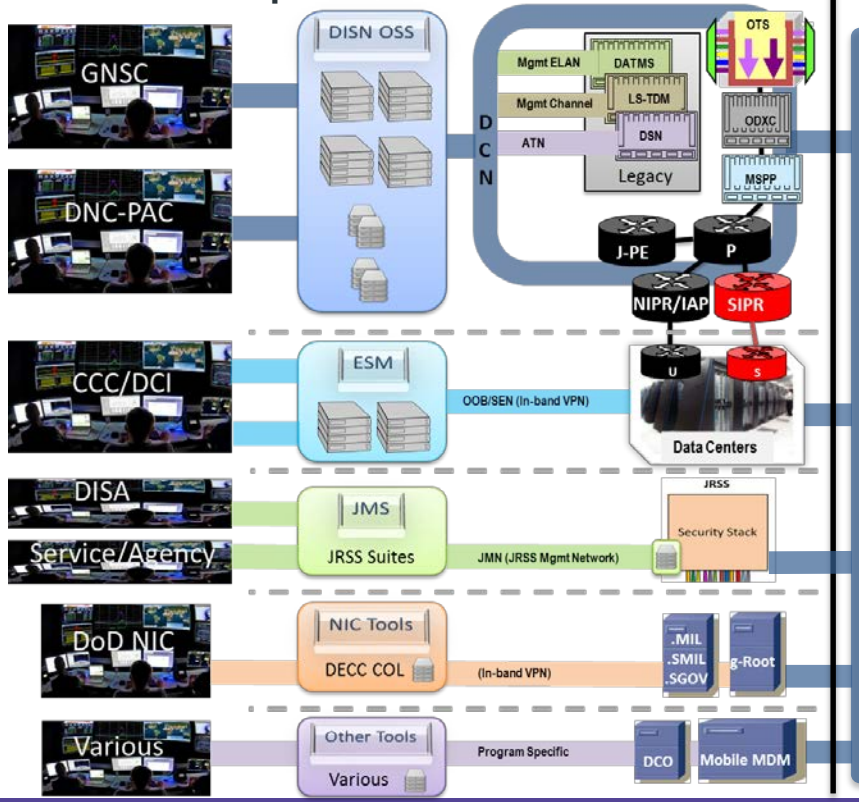
Baseline: Separate Tools & Architectures



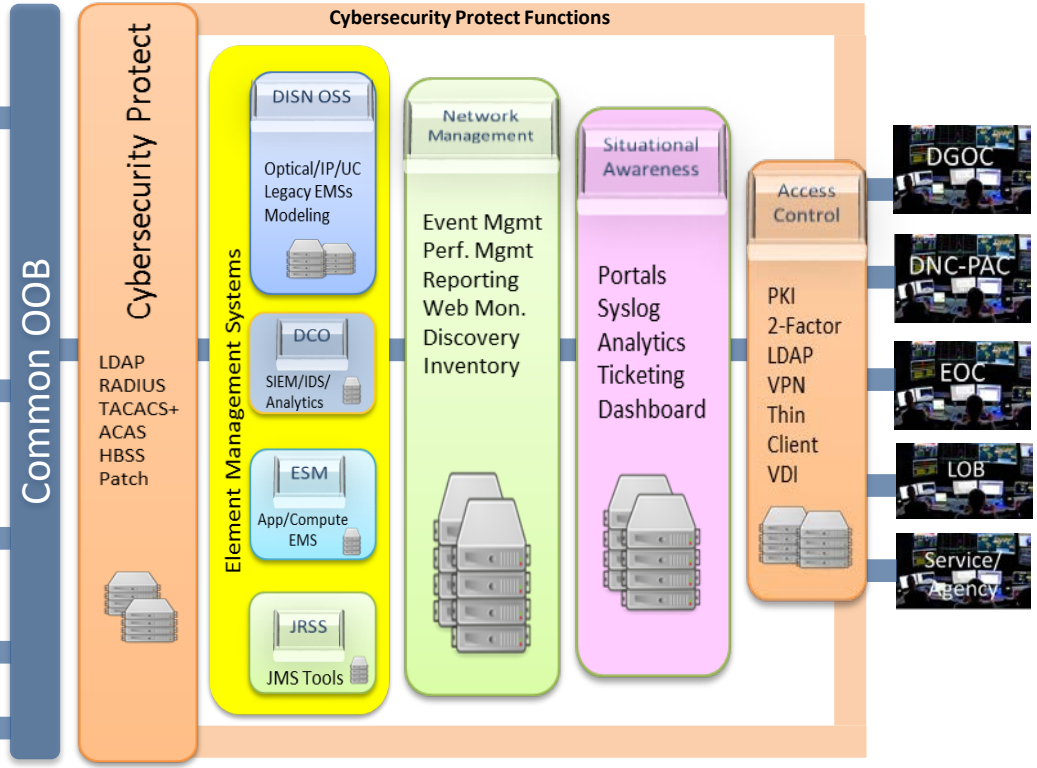
DISA Telemetry & Control - Future

What's the Telemetry Env

Baseline: Separate Tools & Architectures

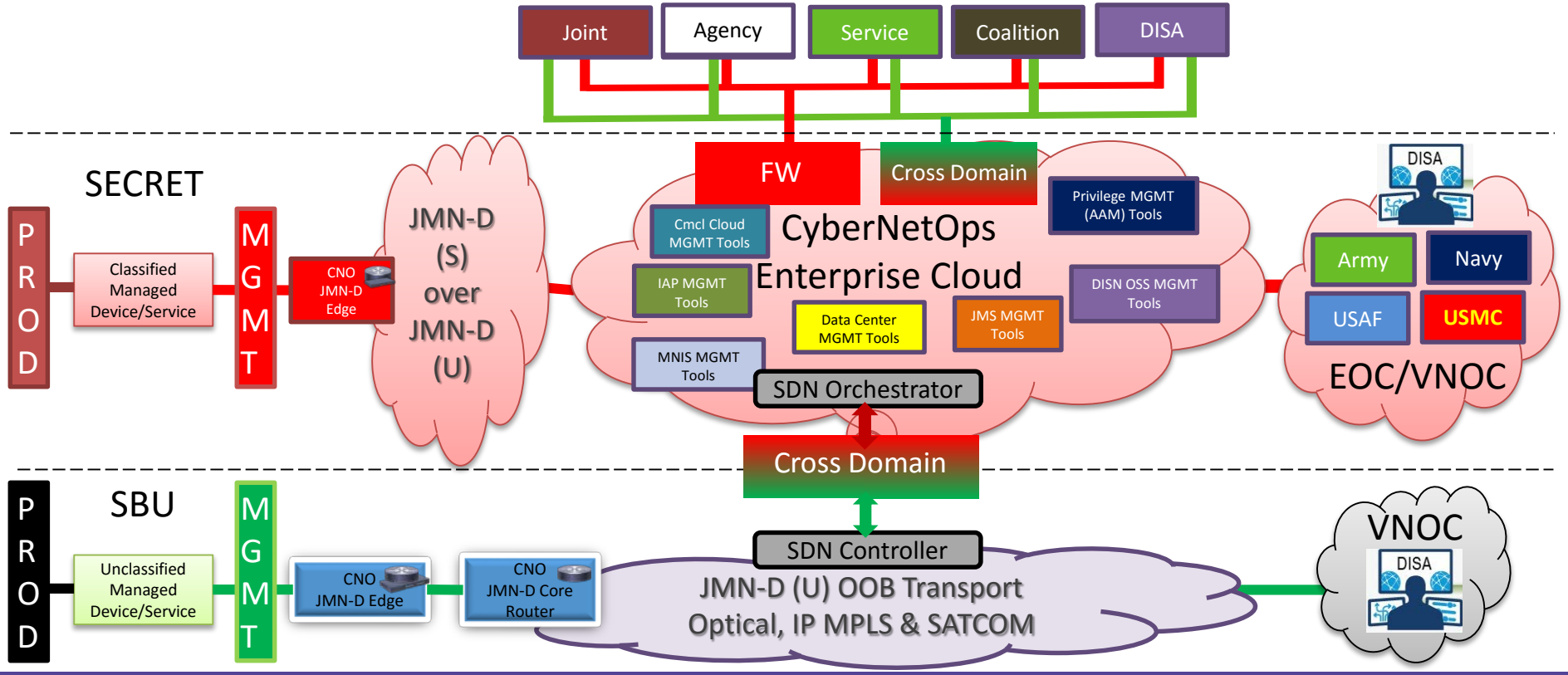


End State: Standard Tools, OPS Views & Architecture



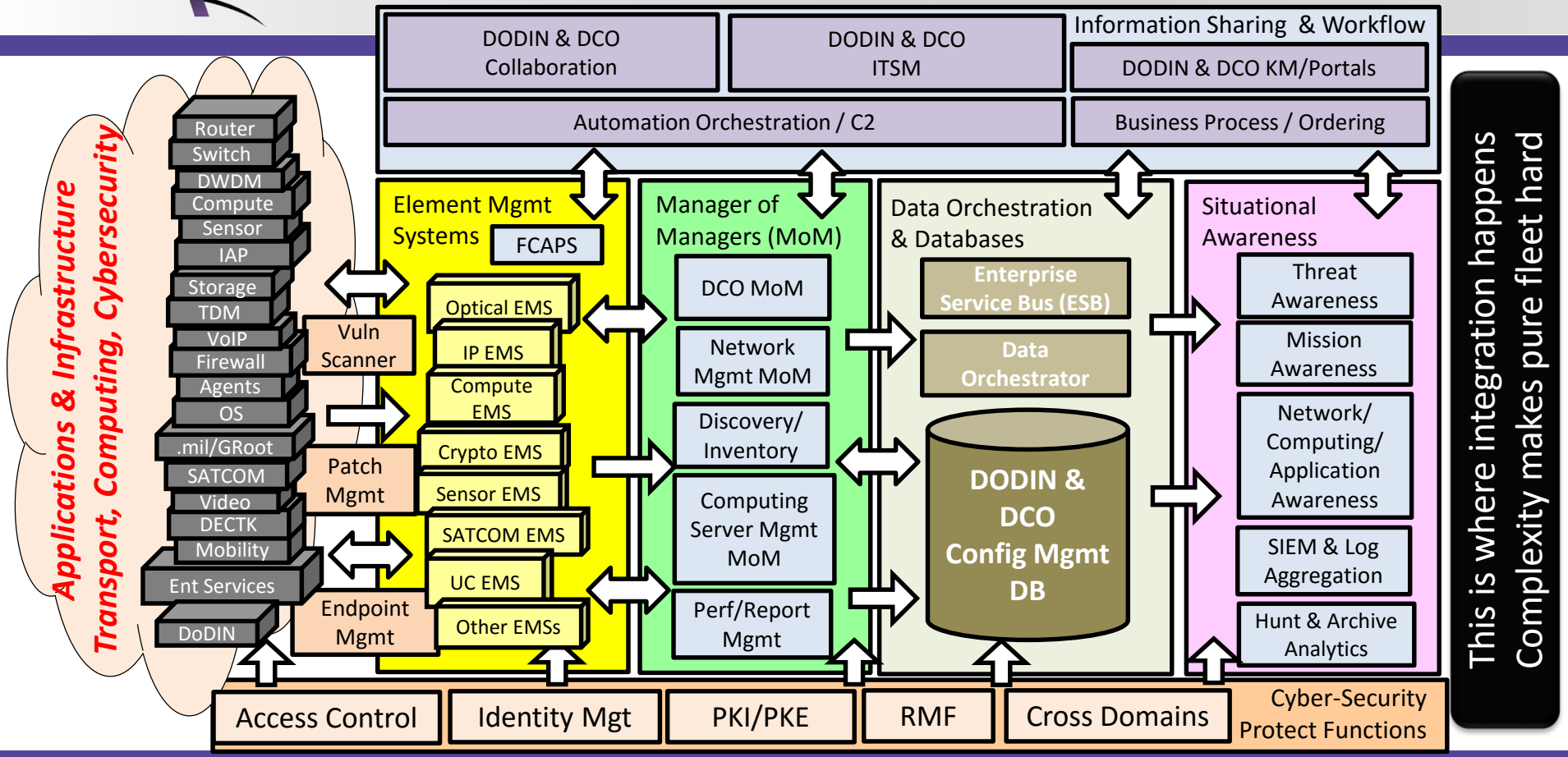
CyberNetOps Enterprise Cloud Architecture

What's the CNO Env



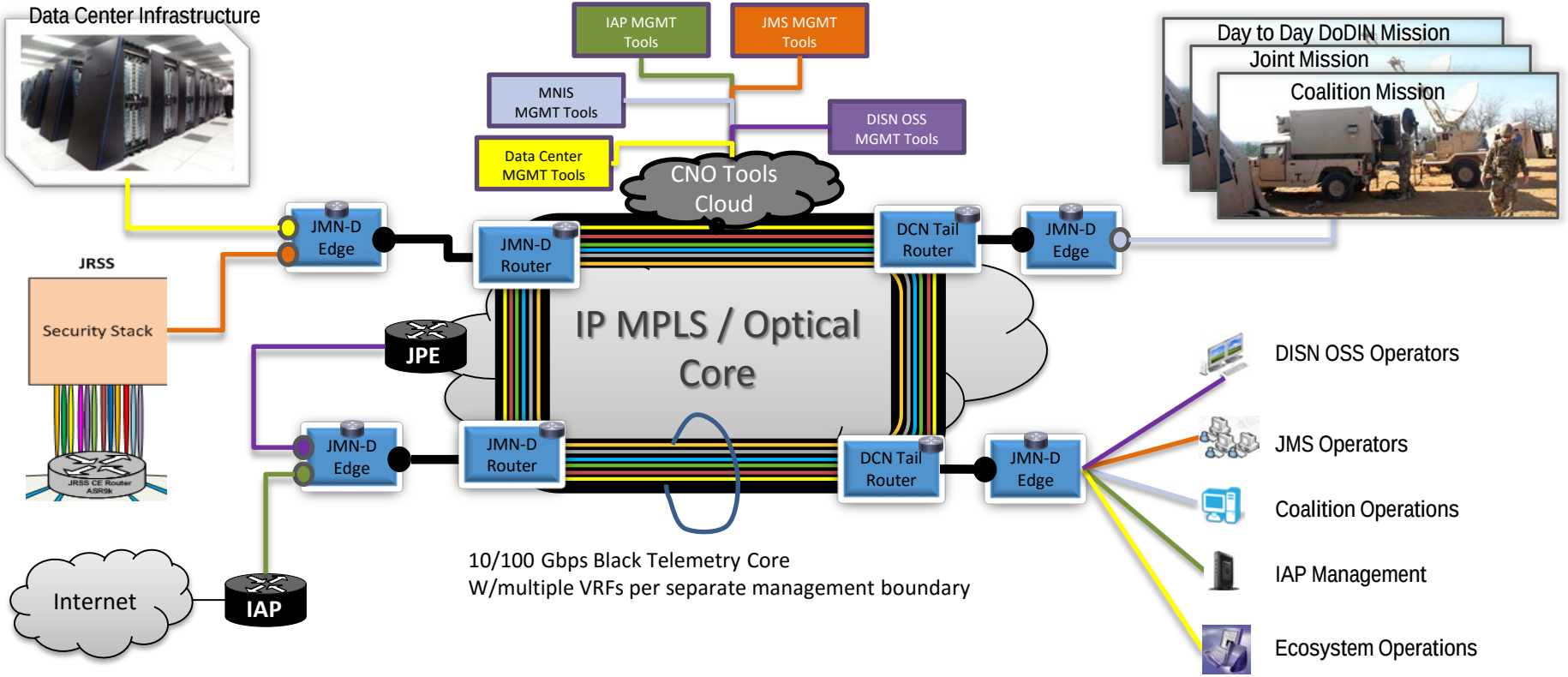
DISA Cyberspace Operations SV-1

What's the CNO Architecture



Future CNO Environment

What's the target CNO Env



rate us

take the **3-question** survey
available on the AFCEA 365 app

visit us

DISA Booth # **443**

follow us

Facebook/USDISA

Twitter/USDISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

Acronyms

AAA	Authentication, authorization, and accounting
ATN	Advanced Defense Switched Network Integrated Mgmt Spt Sys Transport Network
BAS-G	Building Automation System-Global
BDP	Big Data Platform
CCV	Common Communications Vehicle
CEMS	Converged Element Management System
CNO	CyberNetOps
CSAAC	Cyber Situational Awareness Analytical Capabilities
DCN	Data Communications Network
DCO	Defensive Cyber Operations
DDOS	Distributed Denial of Service
DECTK	DISN Enterprise Classifed Travel Kit
DEPS	DOD Enterprise Portal Service
DMCC	Defense Mobility Classified Capability
DNC	DISN NetOps Center
DRSN	Defense Red Switch Network
DSN	Defense Switch Network
DWDM	Dense Wave Division Multiplex
ECVoIP	Enterprise Classified Voice over IP
EMS	Element Management System
EOC	Enterprise Operations Center
ESM	Enterprise Service Management
EVoIP	Enterprise Voice over IP
FOC	Final Operational Capability
FW	Firewall
GVS	Global Video Service
GVS-C	Global Video Service – Classified
IAP	Internet Access Point
IAPNet	Internet Access Point Network
IdAM	Identity and Access Management

ISS	Information Sharing System
ISZ	Information Sharing Zone
ITSME	Information Technology Service Management Enterprise
JMN-D	Joint Management Network-DoDIN
JMS	Joint Management System
JMS	Joint Management System
KM	Knowledge Management
LOB	Line of Business
LS-TDM	Low Speed – Time Division Multiplexer
ME	Managed Element
MNIS	Multinational Information Sharing
MPLS	Multi-protocol Label Switching
NCCM-R	Network Configuration and C hange Management- Replacement
NMS	Network Management System
OOB	Out of Band
OSS	Operational Support System
OS	Operating System
OTS	Optical Transport System
PCAP	Packet Capture
PDR	Preliminary Design Review
PKI	Public Key Infrastructure
PROD	Production
PSC	Production Support Review
SA	Situation Awareness
SDN	Software Defined Networking
SIEM	Security information and event management
UC	Unified Capabilities
VNOC	Virtual Network Operations Center
VRF	Virtual routing and forwarding
WWOLS	Worldwide Online System