Agency Perspective: DoD HPCMP

Dr. Reed L. Mosher – Director, ITL

NSCI: HPC Workshop, 30 September 2016

Overview

- DoD HPCMP Overview
- Drivers for the Future
- Hardware Update
- Software Update
- Networking Update
- Cybersecurity Update
- Cyber Situational Awareness

HPCMP High-Level Operational Concept

Users

DOD HPC DEPARTMENT OF DEFENSE HIGH PERFORMANCE COMPUTING MODERNIZATION PROGRAM

A technology-led, innovation-focused program committed to extending HPC to address the DoD's most significant challenges

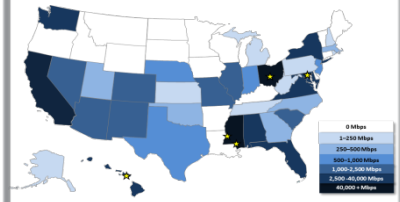
DoD Supercomputing Resource Centers (DSRCs)

- US Air Force Research Laboratory DSRC
- US Army Research Laboratory DSRC
- US Army Engineer Research and Development Center DSRC
- Maui High Performance Computing Center DSRC
- US Navy DSRC

Information-assured Networking

Defense Research & Engineering Network (DREN)

Connects DoD HPC Centers and Users

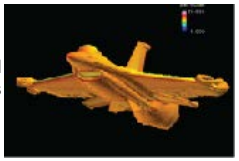


High-bandwidth, Low-latency Full-service Network

Software Applications

Core Software

Computational Environments

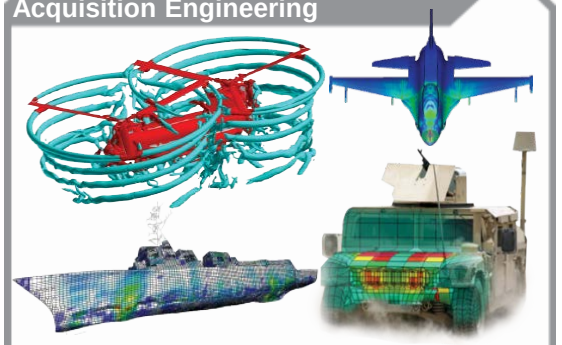


Education and Training

Support

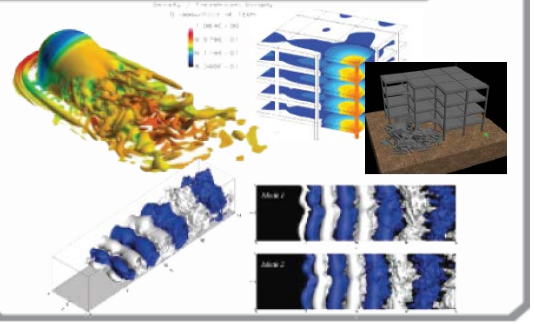
Results

Acquisition Engineering



Decision Support

Science and Engineering Research



HPCMP Highlights

Spans many important use cases which require significant computation and networking capabilities

- **Science and Technology (S&T)**
  - Active HPCMP presence in 53 of 62 DoD laboratories
    - Vehicle aerodynamics, structure, and combustion for hypersonic flight
    - Electromagnetic railgun design
    - Directed energy weapon design
    - Stratified turbulence for submarine design
    - Blast protection for vehicles and occupants
    - Discovery and analysis of new materials
- **Test and Evaluation (T&E)**
  - 20 out of 22 DoD* Major Range and Test Facilities connected to DREN/SDREN. Supported 25 T&E activities in FY15 for Joint Mission Environment Test Capability (JMETC)
    - F-35 Joint Strike Fighter (JSF) Record and Playback
    - Small Diameter Bomb (SDB) II Testing
- **Acquisition Engineering**
  - 116 government and industry organizations use HPCMP software to assess the performance of more than 70 DoD weapon systems
  - Military platform analysis and performance prediction
    - Fixed wing air vehicles, rotorcraft, ships, ground vehicles, antennas, RF signature

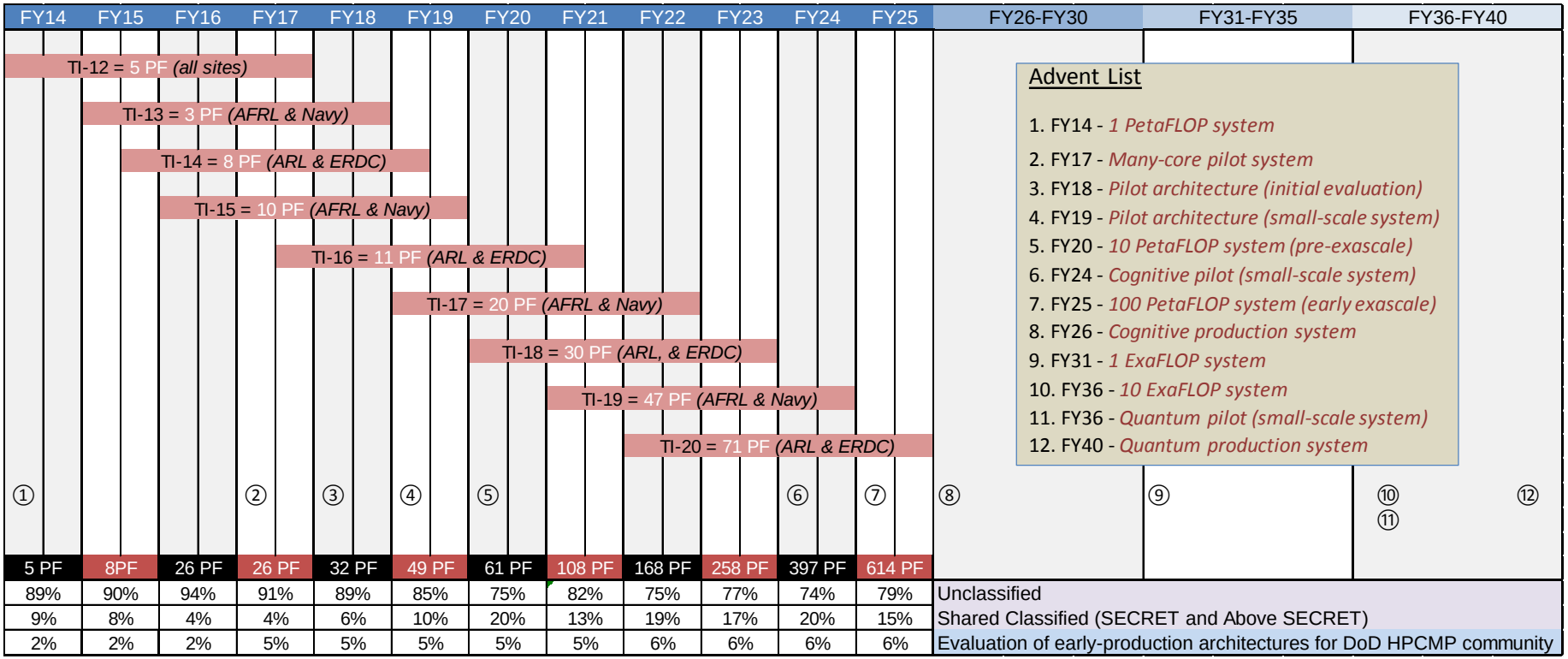
* not connected: 45th Space Wing (Patrick AFB, FL) & 30th Space Wing (Vandenberg AFB, CA)

Drivers for the future

- **S&T, T&E and Acquisition Engineering requirements**
  - **Communities of Interest** and potential **new HPC user communities** that are emerging, e.g., hypersonics, space, electronic warfare, autonomy
  - A focus on addressing challenges for T&E via **HPC-enabled computational proving grounds**
  - **Different workload classes** that require rapid turnaround-time to meet T&E and acquisition program deadlines that necessitate tailoring systems to meet Service/Agency requirements
  - Cost-effective HPC solutions that address the acquisition community and DoD's critical R&D problems may require **shared above-secret computing**
  - The **volume of data** produced by numerical models and T&E events is challenging traditional data management and analysis methods. New data-centric approaches such as **data-intensive computing and decision analytics** are essential to address these challenges
- **Technical HPC challenges**
  - **Increasingly complex** heterogeneous supercomputing **architectures** *(requires code refactoring, new I/O approaches, new algorithms, new resiliency approaches)*
  - **Increasingly complex** physical and engineered **systems** *(requires multi-scale, multi-physics modeling with uncertainty quantification and design optimization)*
  - **Increasingly diverse architectures** (*e.g., data-intensive, cognitive, reconfigurable)*
- **Maintaining a strong cybersecurity posture**

The HPCMP is committed to exploring these with the Services/Agencies.
Prioritization and allocation of HPCMP resources will be identified through high-level Service/Agency strategic engagement.

Hardware Update



- **Balanced investments**
  - Shared classified computing
  - Evaluating early-production architectures for DoD HPCMP community
  - Data analytics for T&E and Acquisition/Engineering communities
  - Data storage infrastructure

HPCMP Supercomputing Centers

DoD Supercomputing Resource Centers

High Performance Computing Modernization Program

MISSION

The mission of the Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP) is to accelerate technology development and transition into superior defense capabilities through the strategic application of high performance computing, networking and computational expertise.

VISION

Our vision is one in which a pervasive culture exists within the DoD that drives the routine use of advanced computational environments to solve the Department's most critical mission challenges.

DoD Supercomputing Resource Centers (DSRCs)

Each DSRC hosts a robust complement of HPC capabilities including: large-scale HPC systems, high-speed networking, multi-petabyte archival mass storage systems, 24x7 operations and customer support services.

Army Research Lab (ARL)
- Classified Computing Services
- Unclassified Computing Services
- Data Analysis and Assessment Center
- Classified Data Recovery

Maui High Performance Computing Center (MHPCC)
- Unclassified Computing Services
- Special Computing Services
- UIT Client Development
- Portal Development

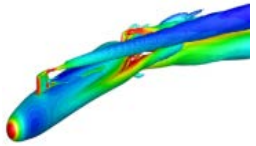
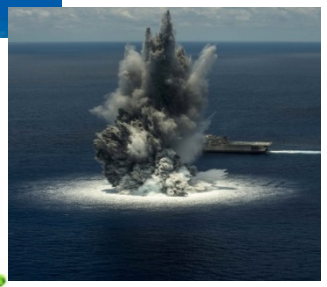
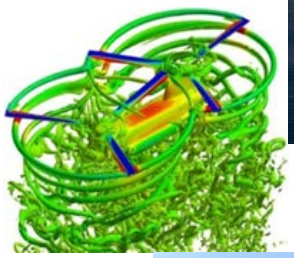
Air Force Research Lab (AFRL)
- Unclassified Computing Services
- CCAC/EUE
- SW Configuration Management
- IAM Panel Lead
- Enterprise Configuration Management and Monitoring

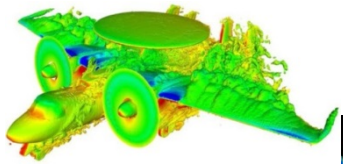
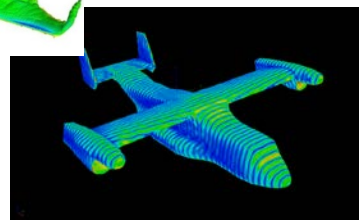
Engineer Research and Development Center (ERDC)
- Unclassified Computing Services
- Open Research Computing Services
- Data Analysis and Assessment Center
- UIT/ezHPC and IE

NAVY DSRC
- Unclassified Computing Services
- Classified Computing Services
- Unclassified Data Recovery

Software Update

- **Computational Research and Engineering Acquisition Tools and Environments (CREATE)**
  - CREATE has been developing and deploying 13 physics-based engineering tools to acquisition engineers (government and industry)
  - CREATE enables DoD engineers to develop and test virtual prototypes of DoD weapon systems.
  - Currently 116 government and industry organizations are using CREATE software to assess the performance of more than 70 DoD weapon systems
- **Must understand and be responsive to acquisition engineering requirements (deadline and event-driven) by providing**
  - Agile allocation of computer resources and job scheduling that accommodates customer workflows, scheduled and unscheduled work, and deadlines
  - Rapid onboarding
  - Easy and secure access to computational resources with ability to run, store, visualize and analyze results
  - Strong protection of intellectual property (codes and data)

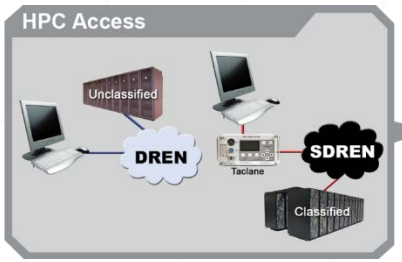
Network & Security High-Level Operational Concept

DOD HPC
DEPARTMENT OF DEFENSE
HIGH PERFORMANCE COMPUTING
MODERNIZATION PROGRAM

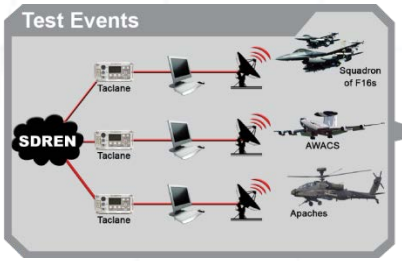
A technology-led, innovation-focused program committed to extending HPC to address the DOD's most significant challenges

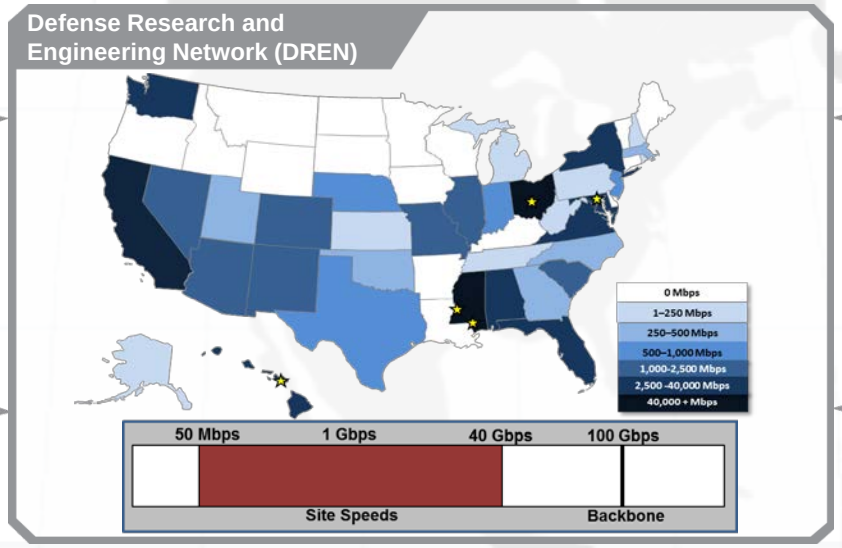
Networking

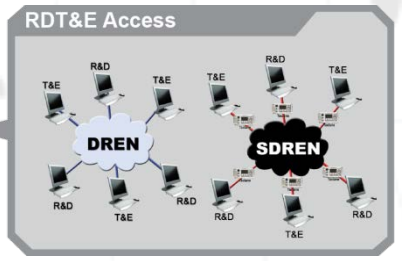
Removes the impact of distance to support the RDT&E community anytime, anywhere with a versatile, low-latency, high-throughput communications network.



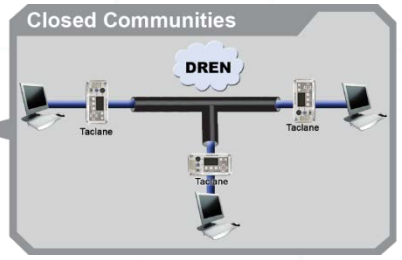
DREN Use-Cases







DREN Use-Cases

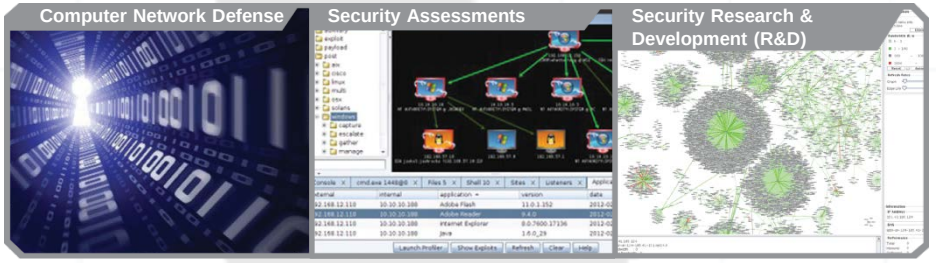


Security

Applies security intelligently to ensure proactive protection while promoting a productive environment for the RDT&E community.

HPCMP Component Security

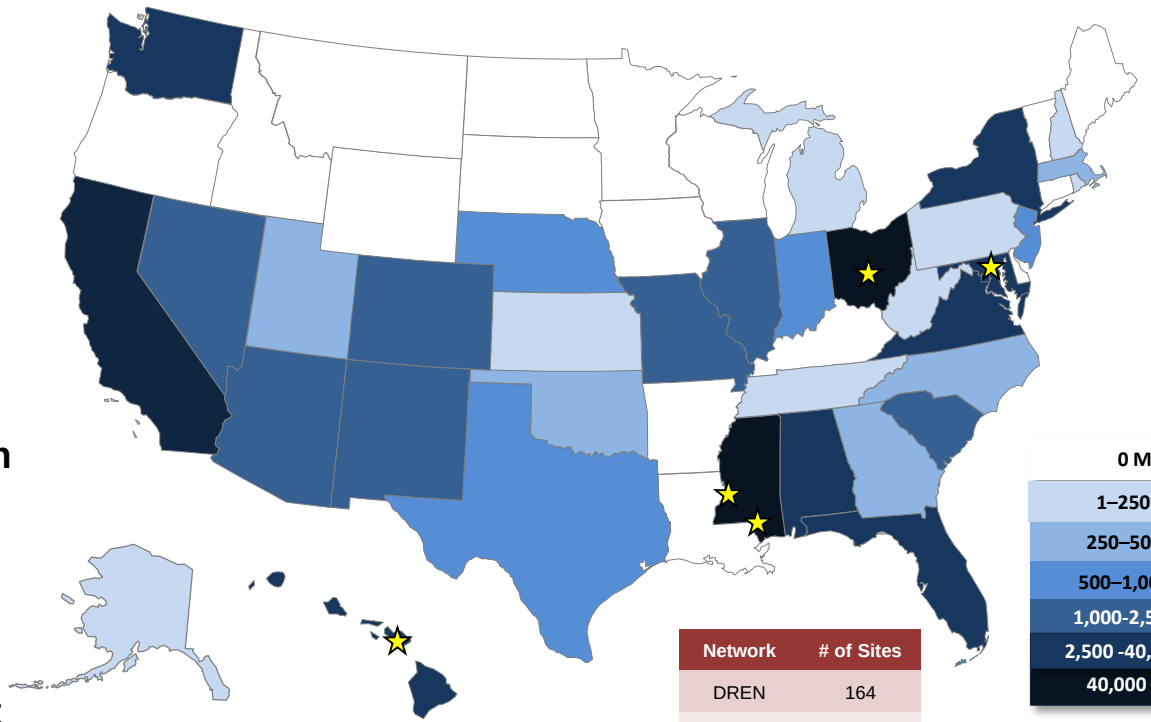
HPCMP Customer Products



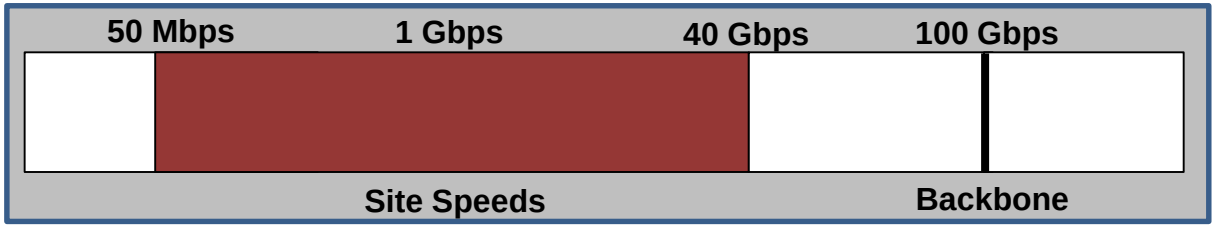
Networking Update

Defense Research & Engineering Network (DREN)

- DoD's premier RDT&E network – focused on S&T and T&E – provides separation from Warfighting networks
- High-bandwidth, low-latency, full-service network
- Connects DoD high performance computing (HPC) centers and users
- Secret-level network overlay on DREN backbone (SDREN)
- DREN III provides 50 Mbps to 40 Gbps service to DoD sites; across a 100 Gbps backbone
- Fully supports IPv6 & Multicast
- Platform for next-generation network protocol and security/ information assurance research
- One component of the DoD Information Networks– RDT&E companion to NIPRNet/SIPRNet

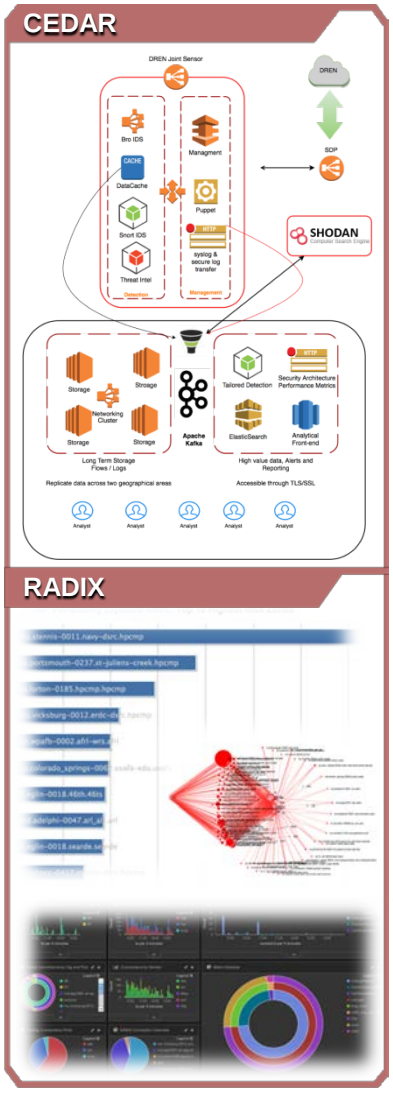


Network	# of Sites
DREN	164
SDREN	71



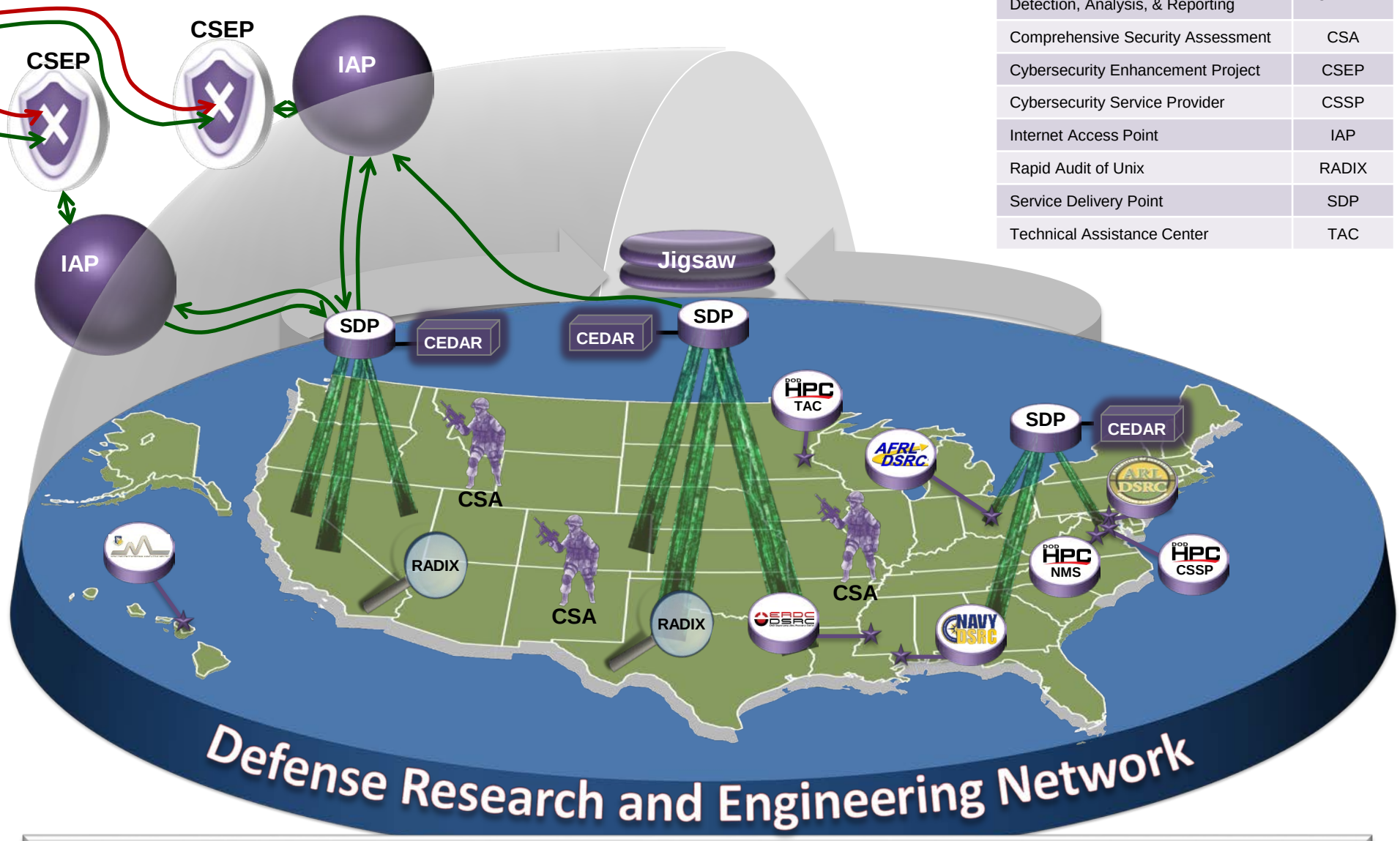
Cybersecurity Update

- **Cybersecurity Environment for Detection, Analysis, and Reporting (CEDAR):**
  - Measures of effectiveness (MOE) framework as independent capability to quantify security performance of cyber defense technologies
- **Rapid Audit of Unix (RADIX):**
  - Host-based scanning capability to effectively support HPCMP's Unix-centric computing environment and provide continuous monitoring capabilities for HPC assets
- **Two-Factor Authentication using YubiKey:**
  - Implementation of YubiKey to enable secure authentication for Researchers and Scientists when accessing HPC assets



HPCMP Cybersecurity OV-1

Cybersecurity Environment for Detection, Analysis, & Reporting	CEDAR
Comprehensive Security Assessment	CSA
Cybersecurity Enhancement Project	CSEP
Cybersecurity Service Provider	CSSP
Internet Access Point	IAP
Rapid Audit of Unix	RADIX
Service Delivery Point	SDP
Technical Assistance Center	TAC



A *defense-in-depth* strategy to intelligently apply security to the RDT&E community

HPCMP Security Architecture

- **Transition to the DoD Risk Management Framework (RMF)**
  - Follows the NIST SP 800-37 and SP 800-53 guidance
  - Follows the 8500 Series Directives/Instructions
  - When RDT&E mission requirements require deviation, mitigations are implemented to provide equivalent protection at an acceptable risk
  - Works closely with DOD working groups to ensure RDT&E needs are represented
- **Monitoring by HPCMP Computer Network Defense Service Provider (CNDSP), a Level III Tier II USSTRATCOM-accredited CNDSP**
  - Level III rating (last validated May 2014) demonstrates “exemplary performance”
  - Actively monitors sensors deployed on DREN at DOD sites & external interfaces
- **Includes an advanced Command Cyber Readiness Inspection (CCRI) called a Comprehensive Security Assessment (CSA)**
  - CSA teams use automated tools to conduct network/host vulnerability scans, penetration tests, configuration reviews and network mapping
  - Continuous monitoring tools provide a risk score based on data gathered from CSA tools, Intrusion Detection Systems and network flows

Cyber Situational Awareness

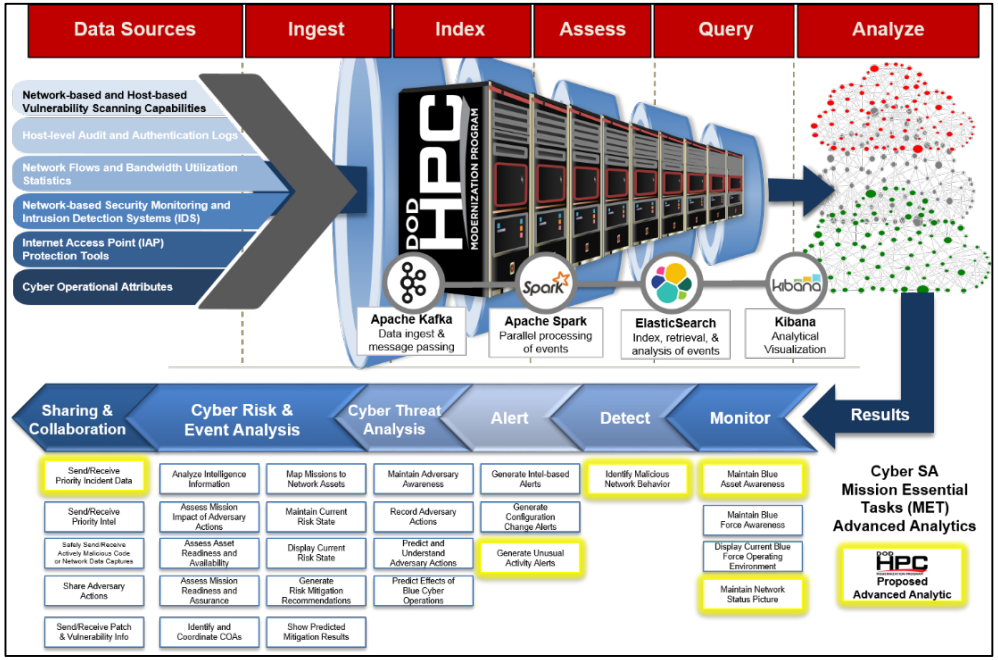
Tasker: Examine applicability of high performance computing (HPC) to cyber situational awareness (SA)

Response:

- ***(FY16)*** **Explore current HPC and cyber SA intersections**
  - Discussed HPC and cyber SA with key members of industry, academia, and government
  - Multiple meetings with Deputy Director, Cyber, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)
  - Establish a rudimentary Spark capability on an HPCMP system
  - Acquired hardware to create initial cyber-data repository
- ***(FY17)*** **Data assembly, ontology, workflow definition, and target/select collaborators**
  - Assemble representative raw cyber-data streams and associated ontology for use by collaborators
  - Develop HPC processing pipeline to minimize data movement and optimize workflow
  - Target and select set of cyber situational awareness collaborators (focused on data analytics)
  - Test feasibility by applying current HPCMP assets to information feeds
  - Initial detection analytics evaluated and pipeline/workflow benchmarks documented
- ***(FY18)*** **Discovery, exploration, and enlightenment**
  - Collaborators perform data analytics studies against static datasets from data repository
  - Collaborators report and document findings
  - Benchmarks are performed comparing HPC solutions with traditional non-HPC solutions
  - End of FY18 will include “Major Decision Point” regarding continuation or modified project objectives

Harnessing HPC for Cyber Situational Awareness

Functional Overview

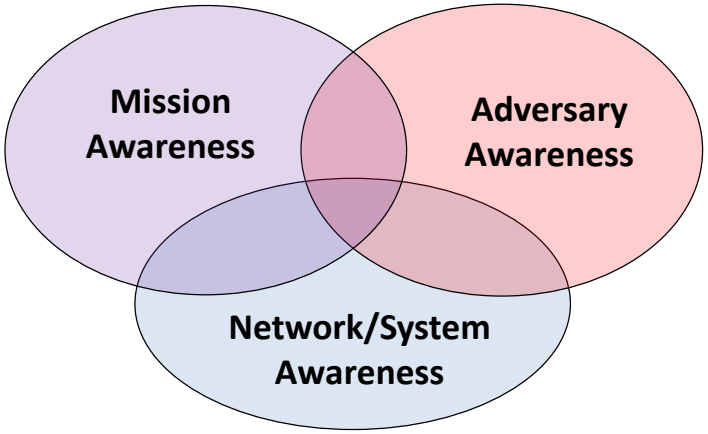


Planned Focus Domains

Approach: Rapidly ingest, index, assess, and query numerous cybersecurity data sources to pursue the following cyber SA advanced analytics:

1. **Maintain Blue Asset Awareness (Monitoring)**
   - Sample Use Case: Pinpoint end-of-life, non-supported systems still connected to networks (i.e. Windows XP, Server 2003, etc.). [Ref. DoD Cybersecurity Campaign]
2. **Maintain Network Status Picture (Monitoring)**
   - Sample Use Case: Classify bandwidth utilization per DREN site to provide awareness of network status and provide indicators of denial of service (DoS) or distributed DoS attacks.
3. **Identify Malicious Network Behavior (Detection)**
   - Sample Use Case: Detection of distributed web vulnerability scanning of public-facing DREN infrastructure.
4. **Generate Unusual Activity Alerts (Alerting)**
   - Sample Use Case: Identify patterns of activity that correspond to core business hours in other known hostile countries.
5. **Send/Receive Priority Incident Data (Sharing & Collaboration)**
   - Sample Use Case: Real-time, machine-to-machine dissemination of indicators of compromise.

Elements of Cyber SA Awareness



The integration of HPC within the cyber workflow will provide:

- **Fusion and assessment of disparate data streams and real time analysis using data science algorithms and machine learning (both structured unstructured data)**
- **Automated, dynamic response mechanisms to significantly reduce the response time to threats (days to minutes)**

Summary

- The HPCMP provides premier high performance computing (HPC) capability to the RDT&E and Acquisition Engineering communities tailored to customer requirements
- A broad range of customer missions are targeted across the DOD
- Strategic engagement with Service/Agency senior leadership to enhance HPCMP linkage with highest mission priorities
- Focus on understanding and supporting new user communities and Communities of Interest, with continued support to current user communities

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu