DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Emerging Technology

Overview

Steve Wallace
Chief Technology Officer
April 26, 2022

DISCLAIMER

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.

DISA Tech Watch List for Fiscal Year 2022 Q3-Q4

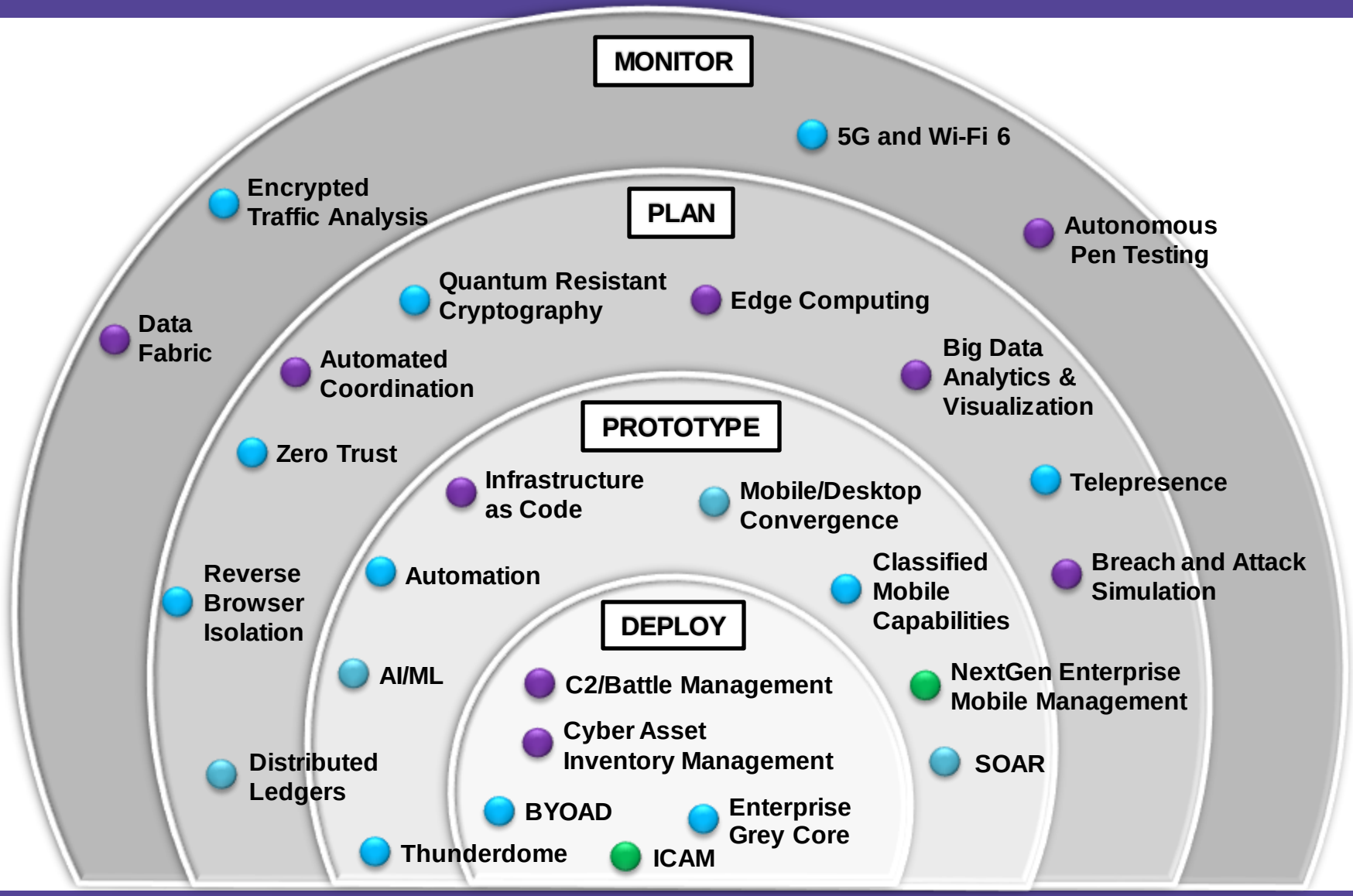
MONITOR: Actively surveying the capabilities and maturity in this area of technical interest.

PLAN: Determining technical impact on DISA and Department of Defense missions. Exploring impacts and integration points within the enterprise.

PROTOTYPE: In process of building or executing.

DEPLOY: Prototype complete and deploying capability to the enterprise.

- **New in FY22**
- **Updated**
- **Existing**



Robotic Process Automation

BUILDING AN RPA PRACTICE

- Effort currently lives in Emerging Technology, will move as it matures
- Total bot count: 55
- DISA Organizations with bots in use today: CFO & PLD
- Leveraging ADVANA platform
- CFO reports 57% reduction in task time, significantly fewer human induced errors

WHAT'S NEXT?

- Greater use of the capability across the agency, ex: operations
- Unattended bots
- Launch of 'Citizen Developer' program

What can **RPA** do?

Perform simple calculations and decisions based on basic logic.

Generate financial reports from applications such as the General Fund Enterprise Business System.

Open, edit or enter data on a web form.

Compare and validate data to support reconciliation requirements.

Extract, collect and input data from the internet, Excel files and databases.

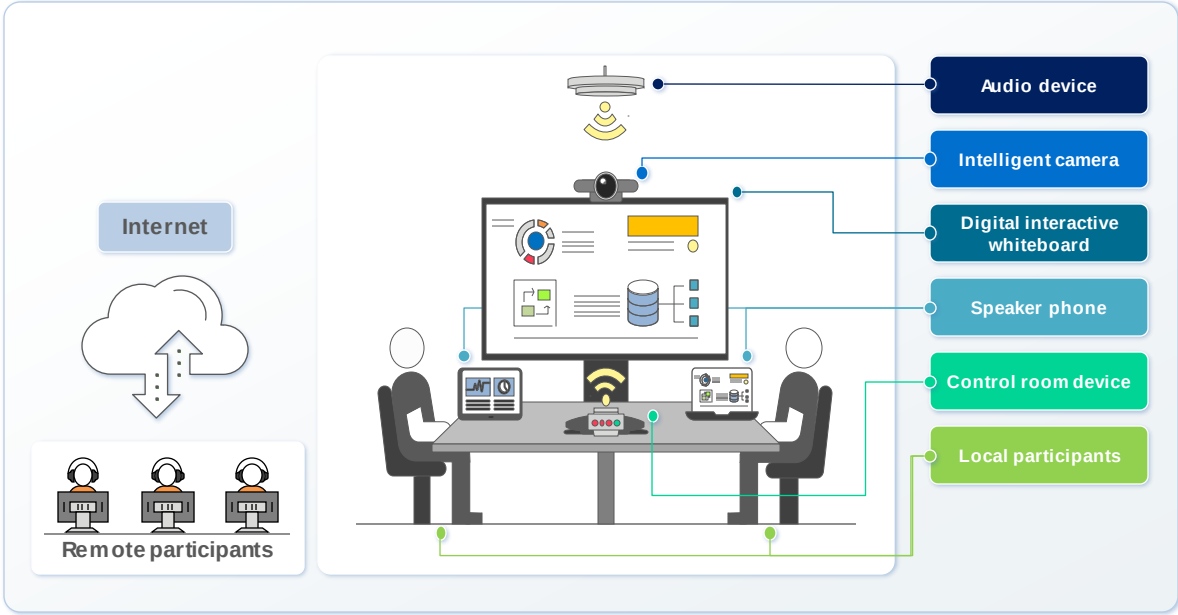
Open and send emails.

NEXT-GENERATION COLLABORATIVE SOLUTION: CHANGING THE LANDSCAPE OF CONFERENCE ROOM MEETINGS

Leveraging the concepts of artificial intelligence, the Defense Information Systems Agency is fundamentally changing the conference room experience to facilitate collaboration among a globally dispersed and mobile workforce. Offered an HD video, audio and content sharing experience, users can join conference sessions, regardless of their location, and contribute and share information in real time.

SMART ROOM CAPABILITIES

- Intelligent conference room control panels connect and manage approved devices as well as cameras and microphones.
- Digital interactive whiteboards allow for editing, saving, printing and sharing content.
- AI algorithms capture whiteboard handwriting and make the material visible even if the user is in front of the shared material.



Quantum-Resistant Cryptography

MITIGATING NEXT-GENERATION THREATS TO DOD NETWORKS

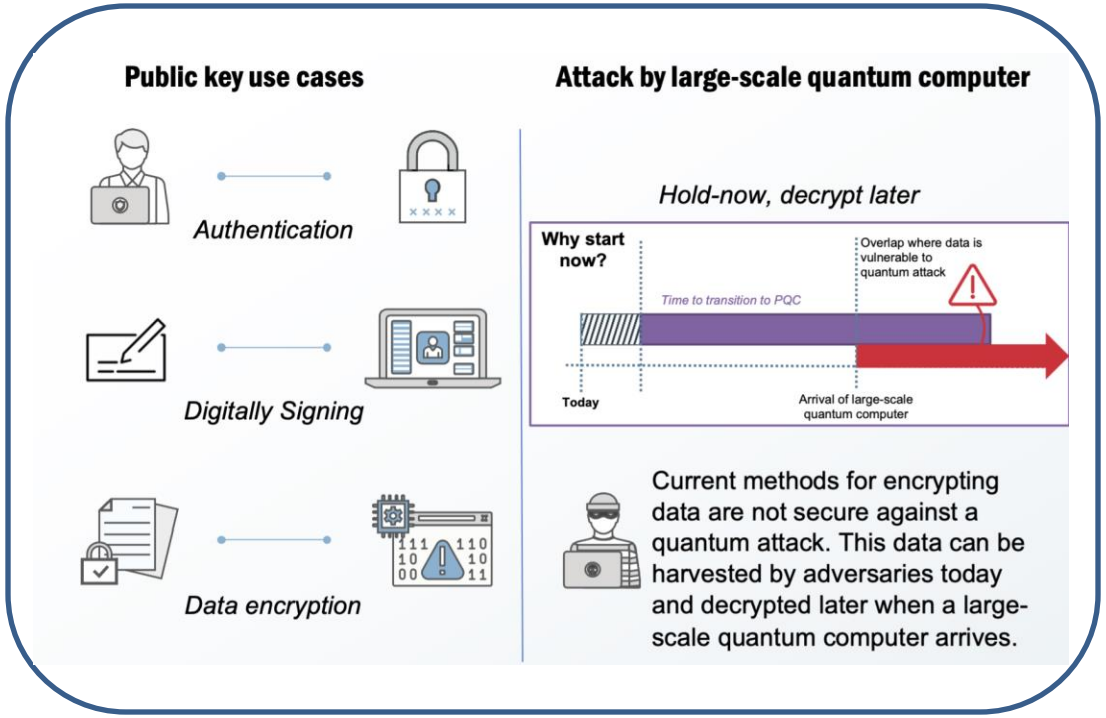
- Quantum computers threaten the DoD landscape by performing calculations far beyond traditional computers
- Present day asymmetric solutions will be unable to protect DoD networks, computers, and data from quantum-based threats
- Adversaries are presumed to be executing harvest now, decrypt later attacks, waiting for quantum computers capable of deciphering the information

DISA'S EFFORTS TO STREAMLINE ADOPTION EFFORTS AND INFORM A MITIGATION STRATEGY

Assess: Agencies must determine which new standards are best tailored to each use case.

Scale: Organizations lack crypto inventory and will need templated processes and procedures to upgrade legacy crypto.

Protect: Organizations must prioritize transition strategies to ensure the most sensitive data is re-encrypted by new standards first.



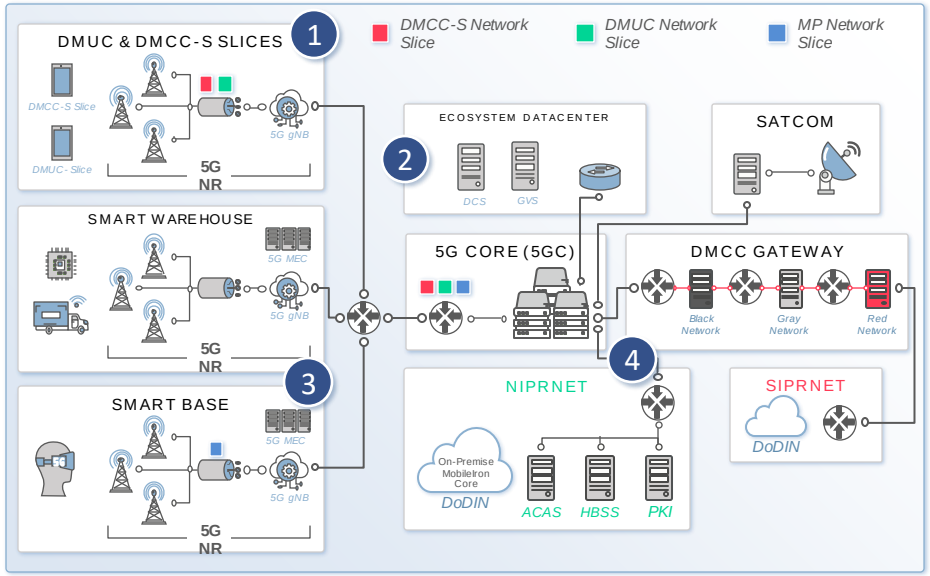
5G Mobility with End-to-End DODIN Security

CONTINOUS MONITORING OF THE LATEST GENERATION OF MOBILE WIRELESS TECHNOLOGY

DISA and U.S. Cyber Command are working to develop a capability for continuous, independent monitoring of non-commercial, government-transiting packet streams for 5G data on frequencies assigned to the DOD to validate the availability, confidentiality, and integrity of the Defense Department's communications system.

THE FUTURE OF UNPRECEDENTED SECURITY

1. Evaluating options to provide Network Slice as a Service (NSaaS) to DMUC, DMCC-S, and mission partners
2. Hosting 5G MEC solutions in HaCC Datacenter to support specific NIPRNet high bandwidth/low latency applications
3. Supporting mission partners in hosting, managing, and security monitoring of private 5G networks for wide range of applications
4. Supporting the 5G NDAA security program across the DoD by recommending and/or implementing Zero Trust Architecture, developing Security Requirements Guide framework, and monitoring USG/DoD requirements



NextGEN CSfC (WINDAR-S)

CLASSIFIED WINDOWS CAPABILITIES

The current WINDAR-S service has become an operational necessity due to COVID-19 and the demand for remote computing and collaboration. DISA's current WINDAR-S service enables a Windows 10-based remote SIPRNet capability. Remote classified capabilities have become a critical component of the modern DOD workforce.

ENHANCED VIRTUALIZATION OF CLASSIFIED MOBILITY

The NextGEN WINDAR-S capability is designed to meet the software virtualization and hardware isolation requirements of the NSA MACP v2.5. NextGEN WINDAR-S will provide users with an enhanced Windows operating environment and secure access to collaborative applications. Data-at-Rest (DAR) protection is provided by layered encryption and optionally, VDI-based non-persistent storage.

DISA's Next-Gen WINDAR-S device baseline will be designed to meet current MACP device architectures.

1. EUD with Inner and Outer VPN Clients in Separate Virtual Machines with a Retransmission Device.
2. Reduce EUD provisioning timelines and operational complexity.

Next Generation Secret Fabric

SECRET FABRIC, TO INCLUDE SIPRNET, IS RIPE FOR CHANGE

- Fabric "Grew Up" vs Designed
- Inconsistent User Experience
- Cloud is likely more disruptive than the Unclassified Fabric
- Fabric has grown, not only horizontally but vertically as well

RETHINKING THE APPROACH

- Collapse of on-prem Directory Services
- Global Gray / GIPRNET
- Integration of ICAM
- More effective partner integration (DMZs)
- More seamless data access, regardless of natively or remotely on network

Enterprise Gray - GIPRNet

CENTRALIZED, REMOTELY-ACCESSIBLE MANAGEMENT NETWORK

DISA is pursuing GIPRNet to fulfill the NSA-developed Enterprise Gray Annex requirements to provide a single centralized management network to support multiple Commercial Solutions for Classified (CSfC) solutions.

ENTERPRISE GRAY MANAGEMENT TO SUPPORT ACCESS FROM MULTIPLE ENTRY POINTS

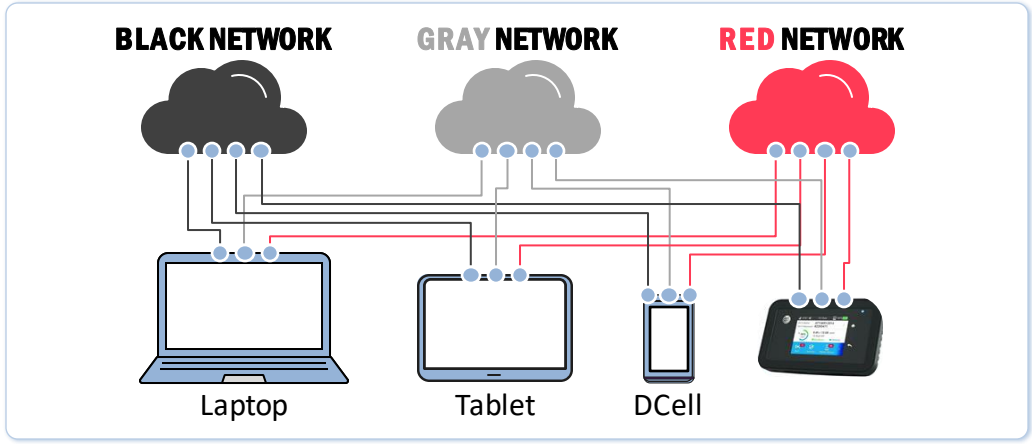
Scalable: GIPRNet Enterprise approach will increase DISA's overall capacity to meet mission partner demand from multiple agencies (e.g. Army, Air Force)

Flexible: GIPRNet will enable DISA and mission partners to leverage CSfC connectivity to adapt to specific mission needs.

Secure: GIPRNet will meet evolving CSfC requirements for Gray Annex, Mobile Access (MACP v2.5) and Multi-Site (MSC v1.1).

Cost Effective: Consolidates and leverage existing systems to provide cost savings.

Efficient: GIPRNet will achieve operational efficiencies by combining/consolidating disparate support approaches.

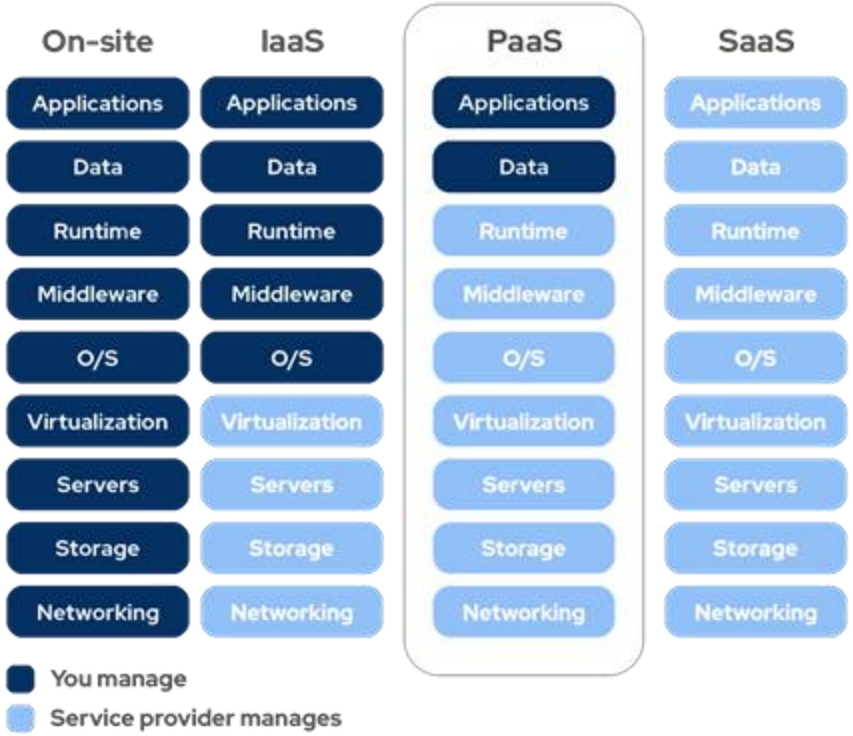


DoD Cloud Infrastructure as Code – Accelerate Cloud Adoption

DoD Cloud IaC are baselines that leverage IaC automation to generate **pre-configured, pre-authorized, Platform as a Service (PaaS)**-focused environments. Whenever possible, DoD Cloud IaC leverages security services offered by cloud service providers over traditional data center tools. DoD Cloud IaC helps customers adopt cloud faster.

Highlights

- **Takes 7 months off typical cloud journey**
  - Baselines for both Azure and AWS, Google in works
  - Supports IL2, IL4 and IL5 workloads. IL6 underway
  - PaaS focused; leveraging CSP Security Tools
- Only decentralized IaC baseline with ATO from DISA RME and Common Controls available for inheritance in eMASS
- Only IaC baseline available in Azure Marketplace
- Only IaC baseline developed under CRADAs w/ CSPs
- We help deploy baselines in a 3-4 hour session for free
- Completed 20 DoD Components deployments



DoD Cloud IaC

Azure

aws

Google Cloud Platform

Data Cataloging Pilot

Current Data Management Challenges:

- Data is unorganized with minimal governance
- Users log in to multiple systems to access data
- Users have limited knowledge and access to available data
- Manual, time-consuming process to request data: User tracks down data steward, who then manually provides access to data

DISA Enterprise Cataloging Service

Data & Metadata (sourcing/ingest):

1. Manual upload
2. Direct connection
3. API

Transformation:

1. Manual
2. Automation (i.e., script)
3. None

AWS Gov Cloud (IL5)

Metadata Discovery, Curation, Tagging, and Cataloging Service

Watson Knowledge Catalog

Cloud Pak for Data

IPS4GRO-as-a-Service

DISA System/Process
WKC metadata integration through API

Business outcomes

1. Classification based data sharing
2. Consistent business definition
3. Data quality improvement for accurate insights

Iterative Curation of Inventory:

Users (i.e., analysts, data stewards, leadership, mission partners) access the data catalog to use and manage data in support of the mission

Pilot Goals:

- Catalogs of curated assets are supported by a governance framework
- One stop shop for metadata
- Fully equipped user accessing DISA's full data arsenal
- Streamlined process by requesting (user) and approving (data steward) data access directly in WKC

Technical Exchange Meetings

CONNECTING GOVERNMENT AND INDUSTRY EXPERTS TO EVOLVE THE DOD IT LANDSCAPE

DISA's Emerging Technology Directorate, in partnership with the office of the DoD Chief Information Officer, hosts weekly technical exchange sessions to connect industry technologists, thought leaders, nonprofit organizations and academia to audiences across the Department of Defense.

PRIORITY AREAS OF INTEREST

- Identity, Credential, and Access Management
- Automation
- Development, security and operations/DevSecOps
- Fifth-generation wireless, or 5G
- Gateway evolution
- Artificial intelligence and machine learning
- Mobile/desktop convergence
- Security orchestration, automation and response, or SOAR
- Zero trust
- Wireless transport

GET INVOLVED

Visit DISA's industry partners website: https://www.disa.mil/en/About/Industry-Partners. Submit a TEM request by emailing your suggestion and contact information to disa.innovation@mail.mil.

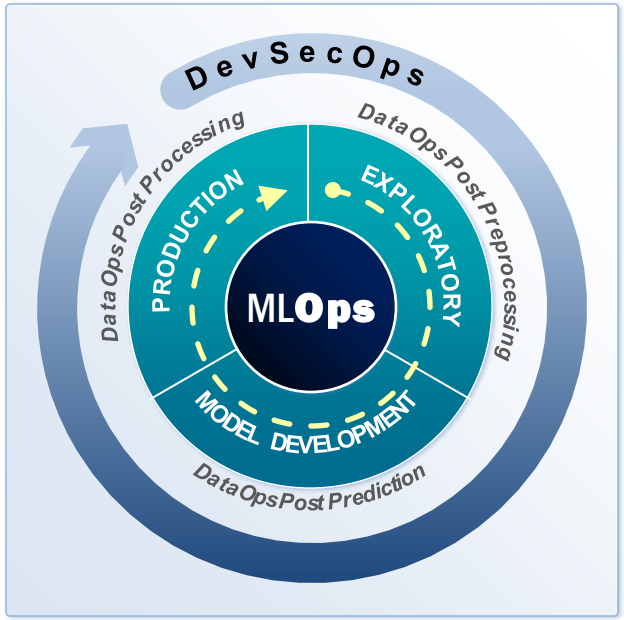
Cooperative Research and Development

TECHNOLOGY TRANSFER AND INNOVATION

The DISA CRADA Program works with DoD-wide organizations to establish collaborative partnerships with industry, academia and other government organizations to accelerate the development and transition of innovative technologies that support joint warfighters and stimulate the civilian economy. CRADA partners may agree to exchange personnel, facilities, equipment, services and other resources to accomplish research, development, testing and evaluation efforts consistent with the agency's mission.

RECENT HIGHLIGHTS

- **DoD Cloud Infrastructure as Code** – DISA's Hosting and Compute Center (formerly known as the Cloud Computing Program Office) has established a CRADA with Amazon Web Service, Google, and Microsoft to design, engineer and deploy secure cloud services, including the cloud virtual networking environment, auditing (centralized logging), least privilege access and authentication.
- **NextTier Concepts Data Operations and Readiness** – NT Concepts specializes in the research, development and operationalization of advanced data analytics, including artificial intelligence and machine learning, specifically supporting DOD and intelligence customers.



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Disa.mil **/USDISA** **@USDISA**