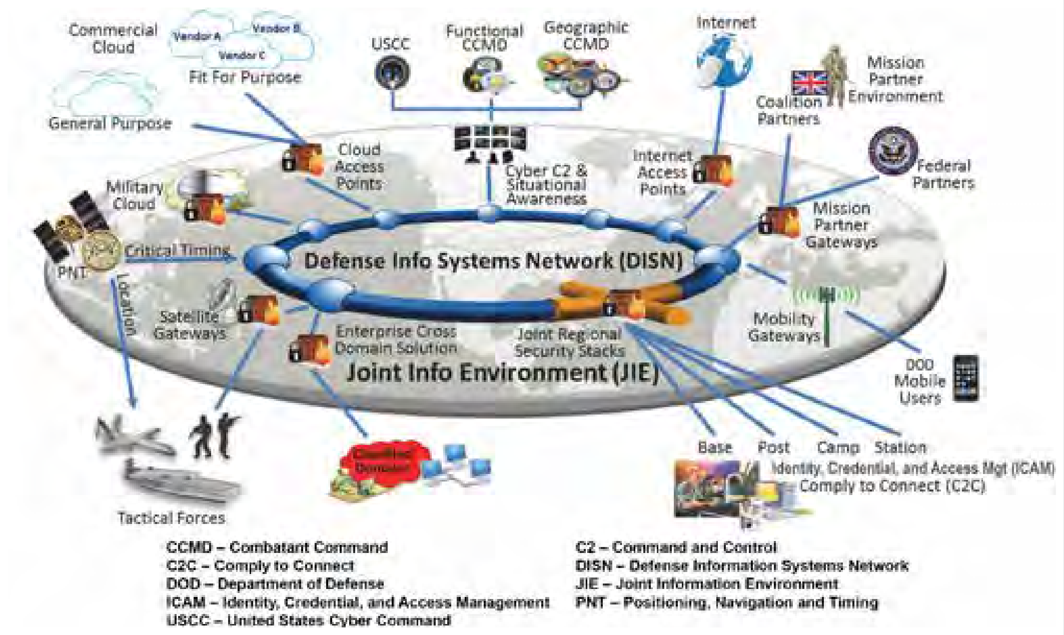
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The DOD Chief Information Officer (CIO), Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve Digital Modernization Strategy (DMS) objectives. Many DMS initiatives use commercial cloud environments and lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. The untested, and therefore unknown, operational performance of DMS programs, projects, and initiatives pose a significant operational risk to the DOD enterprise, particularly in a threat representative, cyber-contested environment. Future deployment decisions need to be informed by adequate OT&E.

System Description

The DOD DMS summarizes the Department's approach to information technology (IT) modernization, focused on the Joint Information Environment Framework intended to improve networking capabilities for fixed and mobile users, institute new enterprise IT services, modernize technology through coordinated refresh efforts, implement a new joint cybersecurity capability, and improve access to data. DOT&E is monitoring the DMS programs, projects, and initiatives that pose a significant operational risk to the DOD enterprise in a cyber-contested environment. These efforts align with the DMS objectives that:

- Deliver a DOD enterprise cloud environment that leverages commercial technology and innovations
- Optimize DOD office productivity and collaboration capabilities, e.g., Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1 (Defense Enterprise Office Solution (DEOS)), Microsoft Office 365 (O365), and ECAPS Capability Sets 2 and 3
- Deploy an end-to-end Identity, Credential, and Access Management (ICAM) infrastructure to support DOD systems
- Transform the DOD cybersecurity architecture, including the Joint Regional Security Stack described in this Annual Report, and initiatives to provide enterprise endpoint security for devices (e.g., desktop and mobile devices)
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE)


Commercial Cloud
Vendor A
Vendor B
Vendor C
Fit For Purpose
General Purpose
USCC
Functional CCMD
Geographic CCMD
Internet
Mission Partner Environment
Coalition Partners
Federal Partners
Cloud Access Points
Cyber C2 & Situational Awareness
Internet Access Points
Military Cloud
Mission Partner Gateways
Critical Timing
PNT
Location
Defense Info Systems Network (DISN)
Satellite Gateways
Enterprise Cross Domain Solution
Joint Regional Security Stacks
Joint Info Environment (JIE)
Mobility Gateways
DOD Mobile Users
Tactical Forces
Base
Post
Camp
Station
Identity, Credential, and Access Mgt (ICAM)
Comply to Connect (C2C)
CCMD – Combatant Command
C2C – Comply to Connect
DOD – Department of Defense
ICAM – Identity, Credential, and Access Management
USCC – United States Cyber Command
C2 – Command and Control
DISN – Defense Information Systems Network
JIE – Joint Information Environment
PNT – Positioning, Navigation and Timing

Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

Programs, Projects, and Initiatives

The DMS is not a program of record. In July 2020, the DOD CIO established the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6 to provide guidance, direction, and oversight of the development, execution, synchronization, and utilization of DOD plans for enterprise IT programs, projects, and other funded initiatives intended to meet the DMS objectives. The DMI EXCOM does not have traditional milestone decision authorities. The DOD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives aligned under DMI EXCOM-approved and Component-funded priorities. DISA is the principal integrator for DOD information network enterprise capabilities, enabling initiatives, and testing. Current Component-funded programs, projects, and initiatives in support of the DMS include:

- **Enterprise Collaboration and Productivity Services (ECAPS)** – In FY20, the DOD established the DEOS acquisition program (ECAPS Capability Set 1) to provide NIPRNET office productivity and collaboration capabilities. In FY21, the DOD, Services, and DISA established DOD O365 commercial cloud environments as replacements for the Commercial Virtual Remote (CVR) environment rather than utilizing the DEOS contract. DISA deviated from the DEOS Phase 1 test approach and focused on fielding the DOD O365 joint tenant environment. The DEOS Program Office and Joint Interoperability Test Command (JITC) failed to update the DEOS NIPRNET Phase 1 Test and Evaluation Master Plan (TEMP) and have yet to develop a DEOS SIPRNET TEMP. DISA is coordinating a contract for ECAPS Capability Set 2 for Business Video and Voice that will be available for future DOD Component use.
- **Identity, Credential, and Access Management (ICAM)** – Based on the draft DOD Enterprise ICAM Implementation Plan, comprises 30+ enterprise capabilities managed by DOD Components intended to create a secure, trusted environment where authorized users can access IT resources. The DOD CIO is the lead for ICAM governance. The current ICAM governance is inconsistent, and the lines of authority remain unclear based on the DOD ICAM Strategy published in FY20. The DOD CIO intends to clarify the roles, responsibilities, and lines of authority for DOD enterprise ICAM capabilities, but has not yet identified a completion timeline. The DOD CIO established Global Directory as the centralized identity and authentication service for the DOD O365 environment and other cloud-based DOD systems.

DISA is developing several ICAM capabilities to support the DOD enterprise and integrating Global Directory with these capabilities. JITC is funded but has yet to conduct T&E of the DISA ICAM capabilities. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.

- **Endpoint Security** is an initiative to better secure endpoint devices. The DOD CIO and DISA published an Endpoint Security Strategy in 2021 that projects deployment of endpoint security capabilities by FY25 to leverage commercial innovation, support cloud adoption, and enable Zero Trust.
- **Mission Partner Environment (MPE)** – The Air Force is acquiring strategic, operational, and tactical MPE services tailored to meet mission partner information sharing needs, which will consolidate and recapitalize 28 physical Combined Enterprise Regional Information Exchange Systems across the DOD. The Air Force conducted an MPE lab-based demonstration in October and November 2021, during EXERCISE BOLD QUEST 21.
- **Enterprise Cloud Efforts** are initiatives intended to leverage commercial cloud innovation for the DOD enterprise to deliver infrastructure and services. DISA fielded military cloud (milCloud) 2.0 in FY19. Due to the unresolved Joint Enterprise Defense Infrastructure (JEDI) protest in 2020, the DOD withdrew from the JEDI contract in FY21 and is developing a Joint Warfighter Cloud Capability multi-cloud vendor contract. The DOD CIO published the DOD OCONUS Cloud Strategy in April 2021.

Test Adequacy

ECAPS – DOT&E conducted ad hoc cybersecurity assessments on DOD O365 tenant environments to inform joint DOD CIO and U.S. Cyber Command fielding decisions in 2021. Due to the accelerated fielding schedule driven by CVR disestablishment in June 2021, these were not comprehensive but still helped identify a range of significant security concerns that the DOD CIO addressed. JITC conducted functional and integration testing of the DOD O365 joint tenant environment; however, the testing was ad hoc and limited in scope.

ICAM – DOT&E conducted an ad hoc cybersecurity assessment of Global Directory in March 2021. The assessment was, however, not a comprehensive evaluation due to the accelerated fielding schedule to support cloud authentication services.

Endpoint Security – DOT&E conducted ad hoc cybersecurity assessments of pilot desktop and mobile device endpoint security solutions in 2021 to reduce risk and gain better understanding of the capabilities to inform future assessments and fielding decisions.

MPE – The Air Force has yet to coordinate with an Operational Test Agency to perform independent T&E for the MPE capabilities.

Enterprise Cloud Efforts – DISA fielded milCloud 2.0 without conducting operational testing of this capability. The milCloud 2.0 contract precludes DOD cybersecurity testing of the hosting infrastructure and some aspects of the environment. Moreover, the DOD has yet to conduct comprehensive, independent, threat-representative cybersecurity testing of any commercial cloud and its hosting infrastructure (to include DEOS and DOD O365), which will require appropriate agreements between the DOD and the commercial cloud service providers.

Performance

There has been little operationally realistic testing performed on DMS programs, projects, and initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability. Many DMS efforts lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. Many DMS initiatives also use commercial cloud environments, but threat-representative cybersecurity testing on the commercial side of cloud environments is not currently being conducted by the DOD.

Recommendations

The DOD CIO, DMI EXCOM, Services, and Director of DISA should:

1. Conduct adequate cybersecurity testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DOD and DOT&E cybersecurity T&E guidance and policy.
2. Perform threat-representative cybersecurity testing of military and DOD commercial cloud environments, to include the commercial infrastructure operated by cloud service providers.
3. Use operational test data, analyses, and reporting to inform DMI EXCOM decisions.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. Develop a TEMP for ECAPS and DEOS, and more generally for each funded DMS enterprise IT initiative.
6. Continue to mature ICAM governance and establish an overarching ICAM program executive to integrate the system efforts and oversee cost, schedule, and performance.
7. Manage the key ICAM capabilities, and all other DMS initiatives, with trained program managers and supporting offices.
8. Develop an overarching ICAM test strategy that encompasses the key issues and concepts to be tested.
9. Designate an Operational Test Agency for MPE and all other DMS initiatives.