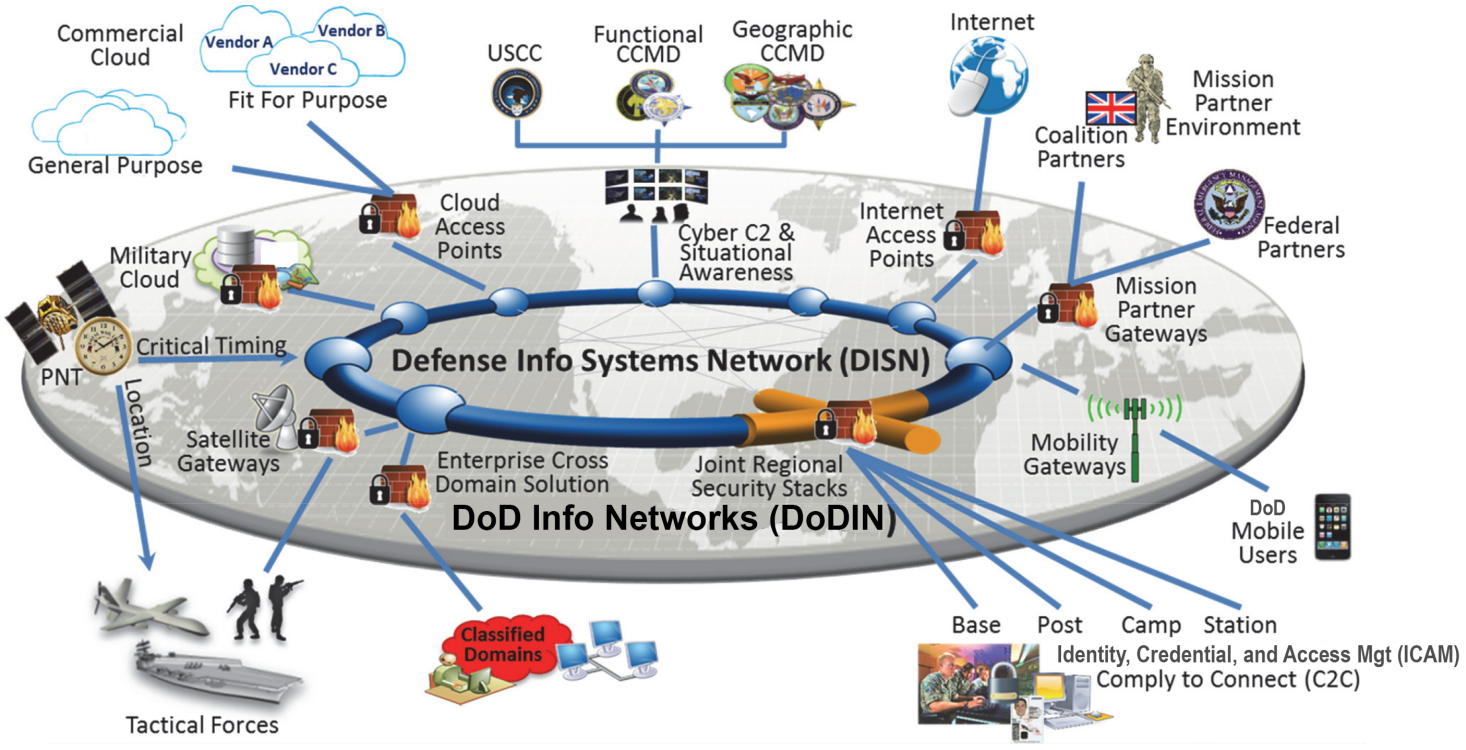
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The DoD Information Enterprise Portfolio Management, Modernization and Capabilities (PM2C) Council continues to govern aspects of the Department's information enterprise to include the Joint Warfighter Cloud Capability (JWCC) oversight and cloud rationalization initiative. In June 2024, the DoD Chief Information Officer (CIO) published the new *Fulcrum: The Department of Defense (DoD) Information Technology (IT) Advancement Strategy.* The Fulcrum Strategy advances the Digital Modernization Strategy (DMS) for the DoD. The DoD CIO, Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DoD DMS objectives. Many DMS initiatives lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance. Deploying untested DMS programs, projects, and initiatives poses an operational risk to the DoD enterprise, particularly in a cyber-contested environment. Future deployment decisions must be informed by adequate OT&E.

SYSTEM DESCRIPTION

The DoD DMS summarizes the Department's approach to IT modernization, focused on the Joint Information Environment Framework intended to improve networking capabilities for fixed and mobile users. The DoD DMS aims to institute new enterprise IT services, modernize technology through coordinated refresh efforts, implement a new joint cybersecurity capability, and improve access to data. Current DoD DMS efforts are intended to:

- 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) via Microsoft Office 365 (O365) on NIPRNet, SIPRNet, and tactical (Denied, Disconnected, Intermittent, or Limited (DDIL)) networks; Capability Set 2 - Business Voice and Video; and Capability Set 3 - Assured Command and Control Voice
- Deploy Identity, Credential, and Access Management (ICAM) capabilities that support DoD systems using a federated approach for DoD-approved Identity Providers
- Transform the DoD cybersecurity architecture to implement Zero Trust throughout the DoD Enterprise, including initiatives to provide endpoint security for devices (both desktop and mobile devices)
- Sustain cybersecurity capabilities to protect the DoD Information Network and support defensive cyber operations and network operations for bases, posts, camps, and stations (known as Joint Regional Security Stack (JRSS))
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE)



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
DoDIN – DoD Information Networks
PNT – Positioning, Navigation and Timing

PROGRAMS, PROJECTS, AND INITIATIVES

In June 2024, the DoD CIO published *Fulcrum: The DoD IT Advancement Strategy*. The Fulcrum Strategy advances the DMS for the DoD. Fulcrum represents the Department's shift towards leveraging technology as a strategic enabler capable of enhancing operational effectiveness and delivering superior value to the warfighter. The DoD CIO intends to establish a governance forum to manage the priorities outlined in the Fulcrum Strategy, track delivery, and focus on resources.

The DoD Information Enterprise PM2C Council continues to govern aspects of the Department's information enterprise to include JWCC oversight and cloud rationalization initiatives. Cloud rationalization is the DoD CIO effort to consolidate the Department's disparate cloud contracts under a single DoD umbrella contract.

DISA is the principal integrator for DoD Information Network enterprise capabilities, enabling initiatives, and testing. Many DMS efforts lack an overarching systems integration process, test strategy, and program structure with trained program managers to manage costs, drive schedules, and monitor performance factors. The DoD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives, which currently include:

- **Enterprise Collaboration and Productivity Services (ECAPS):** In FY24, the DEOS Program Management Office (PMO) continued efforts to provide commercial cloud-hosted SIPRNet office productivity and collaboration capabilities (known as DoD365-Sec) with cyber testing support provided by the Joint Interoperability Test Command (JITC). In FY24, the DoD CIO and DISA continued fielding DoD365 Integrated Phone System (DIPS) on NIPRNet to support ECAPS Capability Set 2 (Business Voice) to the Services and Agencies with projected full deployment in FY25. The DoD needs to address OCONUS and Next Generation 911 dialing in DIPS; however, these enhancements have yet to be funded. DISA is providing ECAPS Capability Set 2 (Business Video) on NIPRNet via DoD365 Teams. In the future, the DEOS Program Office intends to work with the Services to implement tactical DDIL network solutions. In FY21, the DoD CIO and DISA determined the solution for Capability Set 3 (Assured Command and Control Voice) to be the DISA-managed Enterprise Classified Voice over Internet Protocol (ECVoIP) service on SIPRNet. The DoD CIO identified Global Video Services-Classified (GVS-C) and DoD365-Sec as the hybrid solution for Capability Set 3 (Assured Video) on SIPRNet. In FY24, DISA began a GVS-C technical refresh that will continue into FY25.
- **Identity, Credential, and Access Management (ICAM):** The DoD CIO is the lead for ICAM governance for the DoD. The six DoD CIO-approved ICAM solutions are Army, Navy, Air Force, Defense Logistics Agency (DLA), Defense Health Agency (DHA), and DoD Enterprise ICAM. DISA is the service provider for DoD Enterprise ICAM. In FY24, DoD CIO and DISA shifted to a Federated approach for Identity Providers (IdP). DISA intends to build a Federation Hub and integrate the Army, Navy, and Air Force ICAM by the end of FY25, and DLA and DHA ICAM in FY26. The DoD Enterprise ICAM is made up of three capability pillars: IdP, Automated Account Provisioning (AAP), and Master User Record (MUR). In FY24, DISA continued integrating financial and other applications with the ICAM capabilities on NIPRNet that will continue through FY26. ICAM solutions need to support Service and Agency requirements and the Zero Trust activities by FY27. The FY24 National Defense Authorization Act (NDAA) required the DoD to establish an Enterprise ICAM acquisition program of record. However, the DoD CIO and DISA are seeking a waiver from this task. A major part of the ICAM acquisition effort is the Public Key Infrastructure, detailed in a separate section of this Annual Report.
- **Zero Trust:** The DoD is adopting a Zero Trust data-

centric security model intended to provide effective security even if networks or devices are breached by an adversary. Thunderdome is an effort to help the DoD implement Zero Trust principles. DISA awarded a Thunderdome production agreement in 4QFY23 and implemented Thunderdome on NIPRNet at DISA and 4th Estate agencies in FY24. DISA transitioned Thunderdome to a Middle Tier of Acquisition program in FY24 and intends to implement Thunderdome on SIPRNet in FY25.

- **Joint Regional Security Stack (JRSS):** In FY21, the DoD CIO began efforts to phase out JRSS and transition to a Zero Trust security and network architecture. The DoD intends to decommission JRSS by the end of FY27.
- **Mission Partner Environment (MPE):** In support of DoD Directive 5101.22E, the Air Force is developing enterprise MPE services tailored to meet DoD mission partner information sharing needs, while supporting rationalization of existing combatant command MPE capabilities, such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS). The Air Force is developing the Secret and Below Releasable Environment (SABRE) as the first modernized MPE capability platform. JITC is working with the Air Force to develop an MPE SABRE TES. In 1QFY25, the Air Force employed SABRE to demonstrate a federated Enterprise IdP capability for Project Olympus, which is a Joint Staff initiative focused on integrating capability development activities in Bold Quest 24. In FY25, DISA intends to provide real identities via Global Federated User Domain (GFUD) to support Project Olympus. In 4QFY25, JITC intends to conduct an operational assessment of SABRE to support an initial operational capability declaration.
- **Enterprise Cloud Efforts:** The DoD continues to leverage commercial cloud innovations to deliver infrastructure and services for the DoD enterprise. In December 2022, the DoD awarded the JWCC multi-vendor contract designed to meet DoD enterprise cloud requirements. Congress directed the DoD in the FY23 NDAA, Section 1553, to conduct cyber testing of DoD commercial clouds containing classified data.

TEST ADEQUACY

DOT&E is monitoring the DMS programs, projects, and initiatives that could provide significant benefits to the DoD, but also could pose a significant operational risk to the DoD in a cyber-contested environment if not adequately protected. Below are specifics for each:

- **ECAPS:** The DEOS PMO and JITC did not conduct an early operational assessment on DoD365-Sec in FY24 as originally planned and reported in DOT&E's FY23 Annual Report because the PMO decided not to test prior to fielding. However, JITC conducted a cyber assessment of DoD365-Sec and GFUD for SIPRNet IdP in 3QFY24, per a DOT&E-approved cyber test plan. DOT&E observed the cyber assessment. DISA has yet to fund JITC to conduct OT&E of ECAPS Capability Sets 2 and 3.
- **ICAM:** DISA did not fund JITC to conduct operational ICAM capability testing in FY24. In FY24, DISA submitted a service request and intends to fund JITC to resume testing support for the DoD Enterprise ICAM in FY25. The DoD CIO sponsored an ICAM issue paper in FY24 that included some funding for JITC to conduct future DoD Enterprise ICAM and Federation Hub operational testing.
- **Zero Trust:** The NIPRNet Thunderdome capability is designed to address the seven DoD Zero Trust pillars. In late FY23 and early FY24, JITC conducted an early cyber assessment of the NIPRNet Thunderdome capabilities. DISA intends to fund JITC to conduct operational NIPRNet and SIPRNet Thunderdome capability testing in FY25.
- **JRSS:** JITC did not conduct OT&E of JRSS in FY24 but will continue to monitor JRSS until it is decommissioned by the end of FY27.
- **MPE:** The MPE SABRE PMO and JITC did not conduct OT&E

of MPE capabilities in FY24. The PMO and JITC intend to conduct a cyber assessment of MPE SABRE in late FY25.

- **Enterprise Cloud Efforts:** In 3QFY24, JITC conducted a threat-representative cyber assessment of the DoD365-Sec cloud infrastructure, per a DOT&E-approved cyber test plan. This was the first operational cyber assessment of a DoD secure commercial cloud per the FY23 NDAA, Section 1553, which required such testing of DoD commercial clouds containing classified data. DOT&E observed the cyber assessment.

PERFORMANCE

In FY24, except for the DoD365-Sec cyber assessment, there was no operationally realistic testing performed on DMS programs, projects, or initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability. DOT&E intends to publish a classified DoD365-Sec cyber test report in 1QFY25.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the DoD CIO, Services, Director of DISA, and various DMS governance forums should:

1. Manage DMS initiatives with trained program managers and supporting offices.
2. Develop a TEMP or TES for each funded DMS enterprise IT initiative.
3. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
4. Perform threat representative cyber survivability testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DoD and DOT&E cyber survivability T&E guidance and policy, and use operational test data, analyses, and reporting to inform DMS governance decisions.
5. Conduct comprehensive cyber survivability testing of secure cloud environments per the FY23 NDAA, Section 1553.