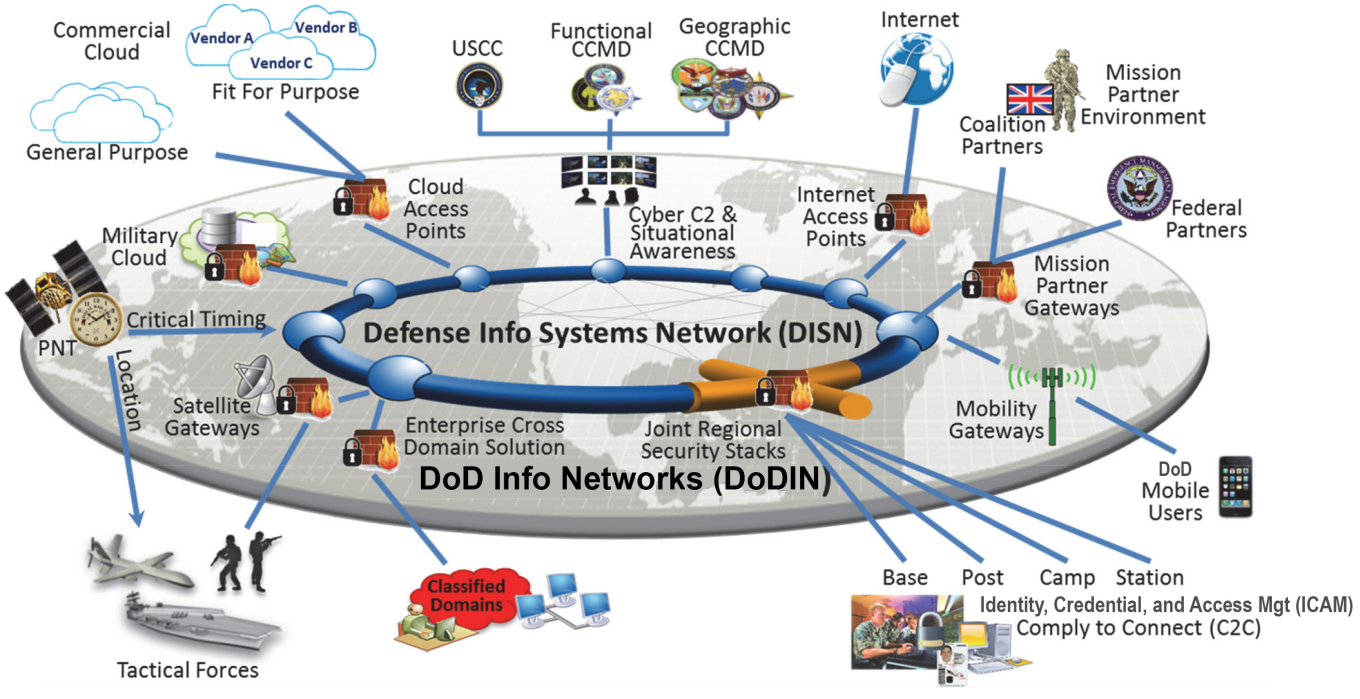
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

In March 2023, the DoD Chief Information Officer (CIO) established the DoD Information Enterprise Portfolio Management, Modernization and Capabilities (PM2C) Council, which it chairs, to govern aspects of the Department's information enterprise to include the Joint Warfighter Cloud Capability (JWCC) oversight and cloud rationalization initiative. This Council superseded the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM). The DoD CIO, Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DoD Digital Moderation Strategy (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 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. 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. 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. 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, tactical, and training networks; Capability Set 2 - Business Voice and Video; and Capability Set 3 - Assured Command and Control Voice
- Deploy an end-to-end Identity, Credential, and Access Management (ICAM) infrastructure to support DoD systems
- 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)
- Implement 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 March 2023, the DoD CIO established the DoD Information Enterprise PM2C Council, which it chairs, to govern aspects of the Department's information enterprise to include JWCC oversight and cloud rationalization initiative. Cloud rationalization is the DoD CIO effort to consolidate the Department's disparate cloud contracts under a single DoD umbrella contract. The PM2C Council convened its first meeting in August 2023. This Council superseded the previous DMS governance structure established in FY20 that consisted of the DMI EXCOM chaired by the DoD CIO, U.S. Cyber Command, and Joint Staff J6. The former Deputy SECDEF approved the DoD DMS in FY19.

DISA is the principal integrator for DoD Information Network enterprise capabilities, enabling initiatives, and testing. The DoD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives. The current funded programs, projects, and initiatives include:

- **Enterprise Collaboration and Productivity Services (ECAPS)** –The DEOS Program Office continued efforts to provide commercial cloud-hosted SIPRNet office productivity and collaboration capabilities (known as DoD365-Sec) with testing support provided by the Joint Interoperability Test Command (JITC). In the future, the DEOS Program Office intends to work with the Services to implement solutions for tactical and training networks. In FY23, the DoD CIO and DISA began fielding DoD365 Integrated Phone System (DIPS) to support ECAPS Capability Set 2 (Business Voice and Video) by FY25. 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.
- **Identity, Credential, and Access Management (ICAM)** – The DoD CIO is the lead for ICAM governance to manage Enterprise ICAM efforts. In May 2023, the DoD CIO published the ICAM Governance Structure and Services memoranda. Enterprise ICAM is made up of three capability pillars: Identity Provider (IdP), Automated Account Provisioning (AAP), and Master User Record (MUR). In FY23, DISA continued integrating financial and other applications with the Enterprise ICAM capabilities on NIPRNet, deployed the Enterprise ICAM IdP on SIPRNet, and piloted Privilege Access Management (PAM) on NIPRNet. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.
- **Zero Trust** – The DoD intends to adopt a Zero Trust data-centric security model that eliminates the idea of trusted networks, devices, personas, or processes and enables authentication and authorization policies under the concept of least privileged access. The DoD CIO published an updated Zero Trust Strategy in September 2022. In 2QFY23, DISA completed development of the Thunderdome prototype, a suite of Zero Trust enabling capabilities that work in concert with existing identity management and cybersecurity tools. DISA awarded a Thunderdome production agreement in 4QFY23 and is implementing Thunderdome on NIPRNet and SIPRNet at DISA and other Defense agencies.
- **Joint Regional Security Stack (JRSS)** – In FY21, the DoD CIO began efforts to phase out JRSS and to transition to a new 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 combatant command existing 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. In May

2023, JITC accepted lead operational test agency (OTA) responsibilities and will work with the Air Force to develop an MPE SABRE test and evaluation strategy (TES). In FY23, the Air Force continued to integrate commercial collaboration capabilities with a National Security Agency-developed Zero Trust architecture to create a DoD-owned and operated cloud environment that will enable secure mission partner information sharing. The Air Force employed SABRE as the U.S. enterprise capability for the MPE Interoperability Initiative 3.0 conducted during Bold Quest 23.2 in September 2023.

- **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 National Defense Authorization Act (NDAA), Section 1553 to conduct cyber testing of secure DoD commercial clouds.

TEST ADEQUACY

- **ECAPS:** JITC intends to conduct an early operational assessment (EOA) on DoD365-Sec in 2QFY24. JITC intends to conduct a cyber assessment of DoD365-Sec and Global Federated User Domain (GFUD) for SIPRNet IdP in 1QFY24, per a DOT&E-approved cyber test plan. JITC supported initial developmental testing on DIPS in FY23. JITC has not been funded to conduct OT&E of ECAPS Capability Sets 2 and 3. In contrast to the FY22 annual report, DISA and JITC are no longer preparing a TES for ECAPS.
- **ICAM:** JITC conducted a developmental cyber assessment on MUR and AAP in a non-production infrastructure in November and December 2022. DISA did not fund JITC to conduct operational ICAM capability testing in FY23 and does not intend to fund JITC in FY24. There is no overarching Program Office or OTA supporting the various ICAM-related initiatives, which has made planning for tests to characterize the overall value and mission impact of the disparate initiatives difficult.
- **Zero Trust:** In January 2023, JITC conducted a limited EOA to assess NIPRNet Thunderdome prototype status toward achieving an operationally effective and suitable determination to inform a DISA fielding decision. The NIPRNet Thunderdome covers four of the seven DoD Zero Trust pillars. In 1QFY24, JITC plans to conduct a cyber assessment of the NIPRNet Thunderdome capabilities. DISA did not fund JITC to conduct operational SIPRNet Thunderdome capabilities testing in FY23 and does not plan to fund JITC in FY24; however, DISA intends to work with JITC to design a future operational test of the Thunderdome capabilities.
- **JRSS:** In May 2023, JITC completed a limited cyber assessment of the final JRSS capability upgrades per a JITC-approved test plan and has no plans for future JRSS testing.
- **MPE:** In January 2023, the Air Force conducted MPE developmental interoperability testing at an Air Force-contracted facility with mission partners.
- **Enterprise Cloud Efforts:** In 1QFY24, JITC plans to conduct threat-representative cyber-OT&E of the DoD365-Sec cloud infrastructure. This is the first cyber-OT&E 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 intends to report the cloud-related cyber test findings in FY24.

PERFORMANCE

In FY23, the DoD CIO's decision to eliminate the DMI EXCOM as the DoD enterprise governance forum for aspects of DMS coordination resulted in less transparency, information sharing, and monitoring of DMS capability dependencies. There has been little operationally realistic testing performed to date 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.

RECOMMENDATIONS

The DoD CIO, Services, Director of DISA, and various DMS governance forums should:

1. Manage the key ICAM capabilities, and all other DMS initiatives, with trained program managers and supporting offices.
2. Designate an OTA for ICAM capabilities and develop an overarching ICAM TES that encompasses the key issues and concepts to be tested.
3. Complete an MPE SABRE TES, and more generally develop a TEMP or TES for each funded DMS enterprise IT initiative.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. 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.
6. Conduct comprehensive cyber survivability testing of secure cloud environments per the FY23 NDAA, Section 1553.