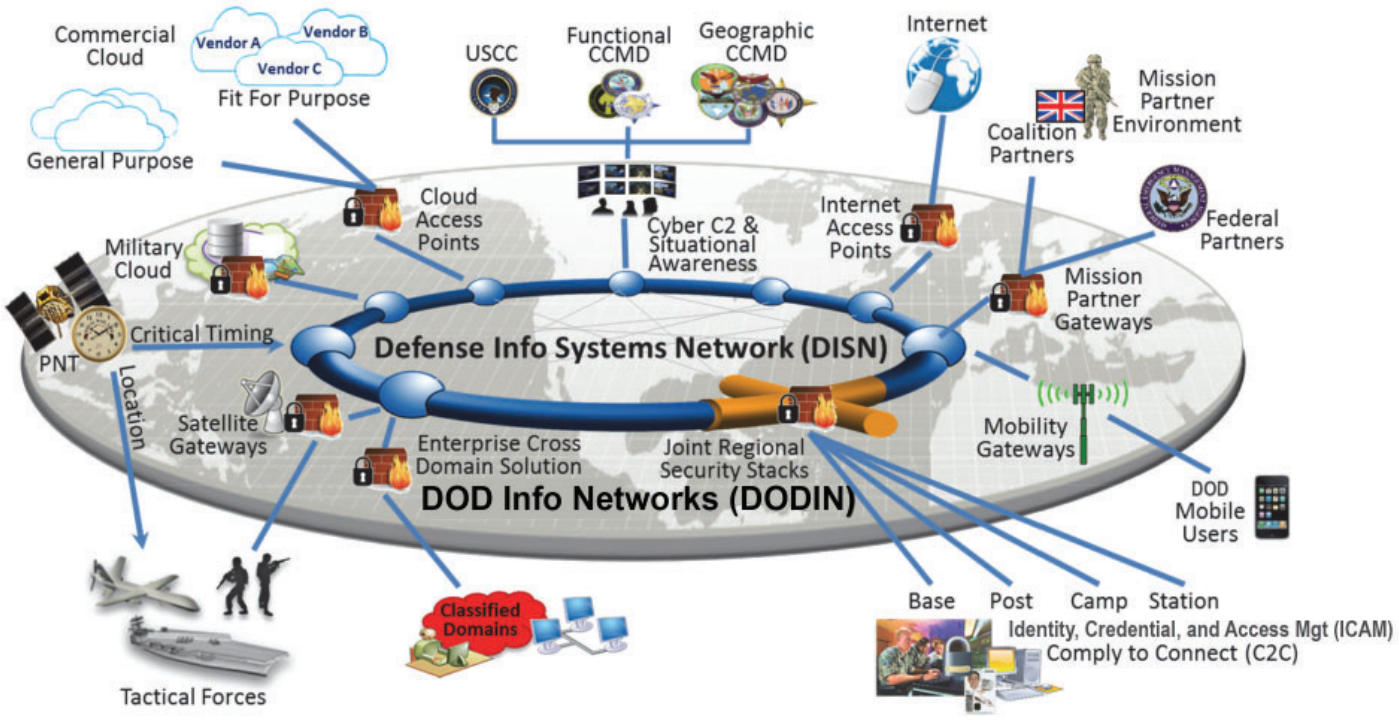
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The former Deputy SECDEF approved the DOD Digital Moderation Strategy (DMS) in 2019. The DOD Chief Information Officer (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 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. These FY22 efforts align with the DOD DMS 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), 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 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 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 FY22, the DEOS Program Office began 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). JITC is developing a Test and Evaluation Strategy (TES) for DOD365-SEC and intends to perform early operational testing in FY23. In FY22, the DOD CIO and DISA reviewed technologies and are finalizing a strategy for DOD users to be provided ECAPS Capability Set 2 (Business Voice and Video) by FY24 and Capability Set 3 (Precedence-based Command and Control Voice) by FY25.
- **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 and intends to establish an ICAM Executive Board to manage Enterprise ICAM efforts. The DOD CIO is clarifying the roles, responsibilities, and lines of authority for DOD enterprise ICAM capabilities. In FY22, DISA developed an enterprise Global Directory Service to provide cryptographic authentication for SIPRNET. In FY22, DISA began integrating several financial application pilots with the DISA ICAM capabilities; this effort will continue and expand to other financial applications in 2023. In FY23, JITC is funded as the operational test agency (OTA) to support DISA ICAM capability testing. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.
- **Zero Trust** is a 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. Zero Trust implementations can repurpose network security to augment data-centric security. The DOD CIO is developing and intends to publish a Zero Trust Strategy in 2023 as well as a companion Endpoint Security Strategy. In FY21, DISA began planning a Zero Trust effort (known as Thunderdome) focused on the network infrastructure. DISA awarded the Thunderdome prototype contract in January 2022. The Services can use Thunderdome or implement their own Zero Trust solutions. JITC is planning to conduct operational testing of the NIPRNET Thunderdome pilot in FY23. DISA intends to begin user migrations to initial Thunderdome capabilities in late FY23. DISA is also working on a new initiative to integrate Thunderdome pilot capabilities with SIPRNET modernization efforts.
- **Joint Regional Security Stack (JRSS)** – Previous testing demonstrated that JRSS could not help cyber defenders withstand threat-representative attacks. In FY21, the DOD CIO began efforts to phase out JRSS and to transition to a new Zero Trust security and

network architecture. JITC did not conduct JRSS operational testing in FY22. In FY23, JITC intends to complete the cyber survivability assessment and an operational assessment of the final JRSS capability upgrades. JRSS is scheduled to be decommissioned by the end of FY27.

- **Mission Partner Environment (MPE)** – In support of DOD Directive 5101.22E, the Air Force is acquiring strategic, operational, and tactical MPE services tailored to meet mission partner information sharing needs, while consolidating existing MPE capabilities, such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS), across the DOD. In FY22-23, the Air Force is integrating 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 is developing a test strategy and intends to conduct future MPE testing in the JITC-sponsored Coalition Test and Evaluation Laboratory with mission partners.
- **Enterprise Cloud Efforts** are initiatives intended to leverage commercial cloud innovation for the DOD enterprise to deliver infrastructure and services. DISA disestablished military cloud (milCloud) 2.0 in FY22 and then established a new government-owned cloud (known as Stratus). Stratus is an on-premise cloud built to meet unique DOD mission requirements. Stratus provides multi-tenant, self-service management capabilities for cloud computing, storage, and network infrastructure. DISA is developing the Joint Warfighter Cloud Capability (JWCC) multi-vendor commercial cloud contract with a projected award date in early FY23.

TEST ADEQUACY

- **ECAPS:** JITC did not conduct any OT&E of the DOD365-SEC capabilities, or the ECAPS Capability Sets 2 and 3 in FY22. JITC and the DEOS PMO intend to conduct an early operational assessment of the DOD365-SEC capabilities in FY23, and they plan to operationally test the ECAPS Capability Set 2 finalized solution prior to fielding in FY24.
- **ICAM:** JITC conducted limited user acceptance testing of the initial DISA ICAM capabilities associated with several financial application pilots in FY22. There was no formal test planning for DISA ICAM capabilities.
- **Zero Trust:** JITC conducted an early operational assessment of Thunderdome pilot capabilities from August to mid-October 2022 to inform a network architecture decision.
- **JRSS:** JITC did not conduct OT&E of JRSS in FY22.
- **MPE:** The Air Force has yet to coordinate with an OTA to perform independent T&E for the MPE capabilities.
- **Enterprise Cloud Efforts:** The DOD has yet to conduct comprehensive, independent, threat-representative cyber survivability testing of any commercial or government-owned cloud and its hosting infrastructure (to include DOD O365, DOD365-SEC, Stratus, and the planned JWCC effort), 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 cyber survivability testing on the commercial side of cloud environments is not currently being conducted by the DOD per the DOT&E memorandum, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, dated April 3, 2018.

RECOMMENDATIONS

The DOD CIO, DMI EXCOM, Services, and Director of DISA 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. Designate an OTA for MPE and develop an MPE TES.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. Develop a TES for DOD365-SEC, and more generally a TEMP or TES for each funded DMS enterprise IT initiative.
6. Conduct adequate 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.
7. Perform threat-representative cyber survivability testing of military and DOD commercial cloud environments, to include the commercial infrastructure operated by cloud service providers.
8. Conduct comprehensive cyber survivability testing of Zero Trust implementations to inform fielding decisions.
9. Use operational test data, analyses, and reporting to inform DMI EXCOM decisions.