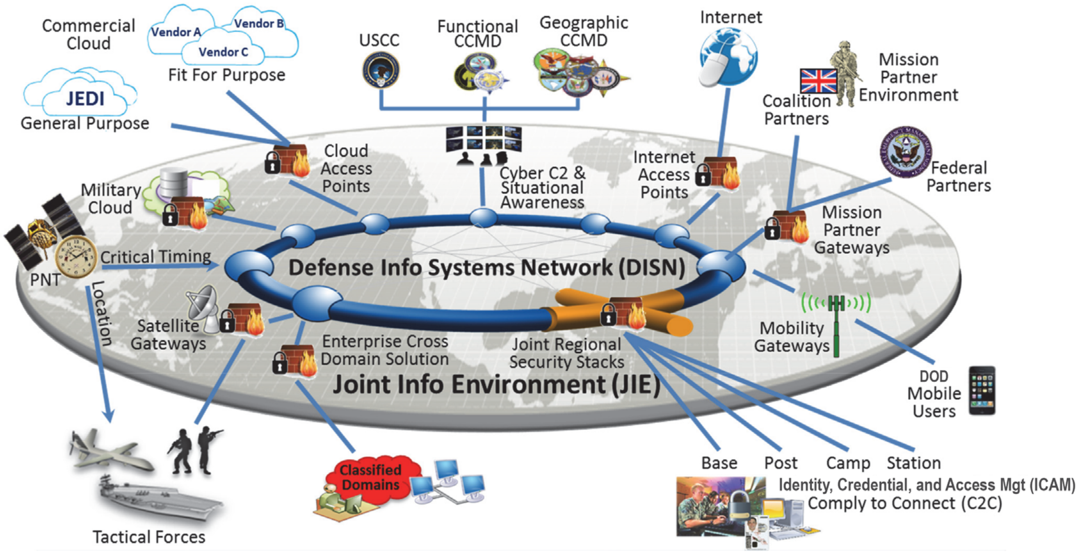
Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives



CCMD – Combatant Command
C2C – Comply to Connect
DOD – Department of Defense
JIE – Joint Information Environment
PNT - Positioning, Navigation and Timing
C2 – Command and Control
DISN – Defense Information Systems Network
JEDI - Joint Enterprise Defense Infrastructure
ICAM – Identity, Credential, and Access Management
USCC – United States Cyber Command

Executive Summary

- In 2020, the DOD Chief Information Officer (CIO) subsumed the Joint Information Environment (JIE) into the broader DOD Digital Modernization Strategy (DMS). The DOD CIO approved the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) Charter that formalized governance, roles, and responsibilities for implementing select strategy elements of the DMS.
- The DOD CIO approved the DOD Identity, Credential, and Access Management (ICAM) Strategy in March 2020 to implement a trusted environment for person and non-person entities to securely access authorized information technology (IT) resources.
- Due to the coronavirus (COVID-19) pandemic, the DOD CIO implemented the Commercial Virtual Remote (CVR) environment as an interim solution to support expanded DOD teleworking from April to December 2020.
- In September 2020, the SECDEF approved the CVR extension through June 2021 under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.
- The DOD and Services are establishing Microsoft (MS) 365 environments as replacements for CVR, and the Defense Information Systems Agency (DISA) intends to establish a DOD 365 environment for the 4th Estate and some Combatant Commands.
- DOT&E continues to stress the need for the DOD to conduct threat-representative cybersecurity testing on commercial cloud platforms to be used by the Defense Enterprise Office Solution (DEOS).

Systems

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE concept as a secure environment, comprising a single security architecture, shared IT infrastructure, and enterprise services.
- The JCS intended JIE to consist of multiple subordinate programs, projects, and initiatives managed and implemented by DISA and the Military Services.
- In January 2017, the JIE EXCOM approved 10 JIE capability objectives.
- In 2020, the DOD CIO realigned JIE with the DOD DMS and mapped the JIE capability objectives executed under the auspices of JIE EXCOM to the relevant DMS elements.
- In July 2020, the DOD CIO chartered the DMI EXCOM to provide oversight of the DMS elements below:
  - Modernize Warfighter Command, Control, Communication, and Computer Infrastructure and Systems
  - Modernize Defense Information Systems Network Transport Infrastructure
  - Modernize and Optimize DOD Component Networks and Services
  - Shift from Component-Centric to Enterprise-Wide Operations and Defense Model

- Strengthen Collaboration, International Partnerships, and Allied Interoperability
- Optimize Data Centers Infrastructure
- Transform the DOD Cybersecurity Architecture to Increase Agility and Strengthen Resilience
- Ensure Cybersecurity Risks are Planned for and Managed Throughout the Acquisition Lifecycle
- Expand the Use of Proven Software and Hardware Assurance Methods
- Deliver a DOD Enterprise Cloud Environment to Leverage Commercial Innovation
- Deploy an End-to-End ICAM Infrastructure
- Improve Information Sharing to Mobile Users
- Improve IT Category Management
- Optimize DOD Office Productivity and Collaboration Capabilities (Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1)
- Optimize DOD Voice and Video Capabilities (ECAPS Capability Sets 2 and 3)

- DMS is not a program of record, and the DMI EXCOM does not have traditional milestone decision authorities. DMS elements are addressed through Service and DISA programs of record and other funded initiatives.
- The DOD CIO is the overall lead for DMS efforts with support from the DMI EXCOM – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6. The EXCOM provides guidance, direction, and oversight of the development, execution, and utilization of DOD enterprise infrastructure. DISA is the principal integrator for DOD Information Networks enterprise capabilities, enabling initiatives, and testing.
- DOT&E is concerned with the cyber survivability of DMS initiatives and less so with their operational effectiveness and suitability.

Activity

Overall

- For the Joint Regional Security Stack updates, see the article on page 37.
- In 2020, the DOD CIO subsumed the JIE into the broader DOD DMS.
- In July 2020, the DOD CIO approved the DMI EXCOM Charter that formalized governance, roles, and responsibilities for implementing select strategy elements of the DMS.
- The DMI EXCOM continued to provide guidance and direct the implementation of the funded initiatives supporting the DMS for the DOD.
- In 2020, the DOD CIO added DOT&E, the Principal Cyber Advisor, and the USD(R&E) as DMI EXCOM members.

ECAPS

- The General Services Administration awarded the DEOS Blanket Purchase Agreement in October 2020.
- Due to COVID-19, the DOD CIO implemented the CVR environment as an interim solution to support expanded DOD teleworking from April to December 2020.
- In September 2020, the SECDEF approved the CVR extension through June 2021 under the CARES Act.
- The DOD and Services are establishing MS 365 environments as replacements for CVR, and DISA intends to establish a DOD 365 environment for the 4th Estate and some Combatant Commands.
- In coordination with the DOD CIO, the USD(A&S) is evaluating and refining the ECAPS capability sets 2 and 3 requirements through 2020.
- DOT&E is coordinating a cybersecurity risk assessment of four Service-led Zero Trust Office 365 Pilot efforts to help inform the Zero Trust technology options for the DOD Federated Office 365 effort. The Zero Trust concept potentially provides significant cybersecurity improvements, if implemented properly.

End Point Security

- In 2020, the Joint Interoperability Test Command (JITC) plan to evaluate two suites of end point security capabilities for DMI EXCOM decision was delayed due to lack of Service support.
- In October 2020, JITC halted the end point security operational assessments to support MS 365 pilot testing.

ICAM

- In March 2020, the DOD CIO approved the DOD ICAM Strategy to implement a trusted environment for person and non-person entities to securely access authorized IT resources.
- The DOD CIO established the Joint Program Integration Office to coordinate ICAM efforts across the Department and with Services and Agencies.
- In June 2020, DISA awarded the ICAM enterprise pilots contract.

Mission Partner Environment (MPE)

- In March 2020, the Under Secretary of Defense for Intelligence and Security, DOD CIO, and Joint Staff issued guidance for information sharing with mission partners in support of globally integrated operations. The MPE capability framework is intended to be used by the U.S. Joint Force to share information with mission partners from the strategic to the tactical levels.
- The DOD CIO is updating the overarching MPE governance policy in 2020/2021.
- The intent is to rationalize and modernize the overall MPE portfolio of command and control, and intelligence information sharing capabilities.
- MPE is intended to consolidate and recapitalize 28 physical Combined Enterprise Regional Information Exchange Systems across the DOD, providing virtualized enduring and episodic MPE services tailored to meet mission partner information sharing needs.

Assessment

- The DOD CIO, DISA, and Services intend to achieve the DMS objectives through implementation of enabling initiatives aligned under the DMI EXCOM approved and funded priorities.
- The DEOS schedule was delayed due to contract award problems in FY20 and by DOD efforts to implement a commercial cloud Impact Level (IL-5) federated environment, due to COVID-19.
- Because the DEOS program plans to use commercial cloud platforms to store classified and unclassified data, it will be critical for the DOD to conduct threat-representative cybersecurity testing on the commercial cloud and its hosting infrastructure. This will require appropriate agreements between the DOD and chosen cloud service providers.
- The DOD, DISA, and JITC lack a funded and consolidated test forum for addressing DMS enterprise information technology initiatives.

Recommendations

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

1. Conduct thorough cybersecurity operational testing of all DMS enterprise initiatives, including threat-representative testing of the commercial cloud capabilities employing current cybersecurity testing guidance and policy.
2. Use operational test data, analyses, and reporting to inform DMI EXCOM decisions.
3. Institute and facilitate remote testing capabilities as a requirement for DMI EXCOM-sponsored efforts to facilitate adequate testing under COVID-19 restrictions.
4. Update the DEOS Test and Evaluation Master Plan (TEMP) based on the contract award and the master schedule for the planned NIPRNET and SIPRNET deliveries.
5. Develop a TEMP for ECAPS current and future capability sets 2 and 3, and more generally for each funded DMS enterprise initiative.
6. Fund JITC to fully support DMS enterprise initiatives, testing, and test-related forums.