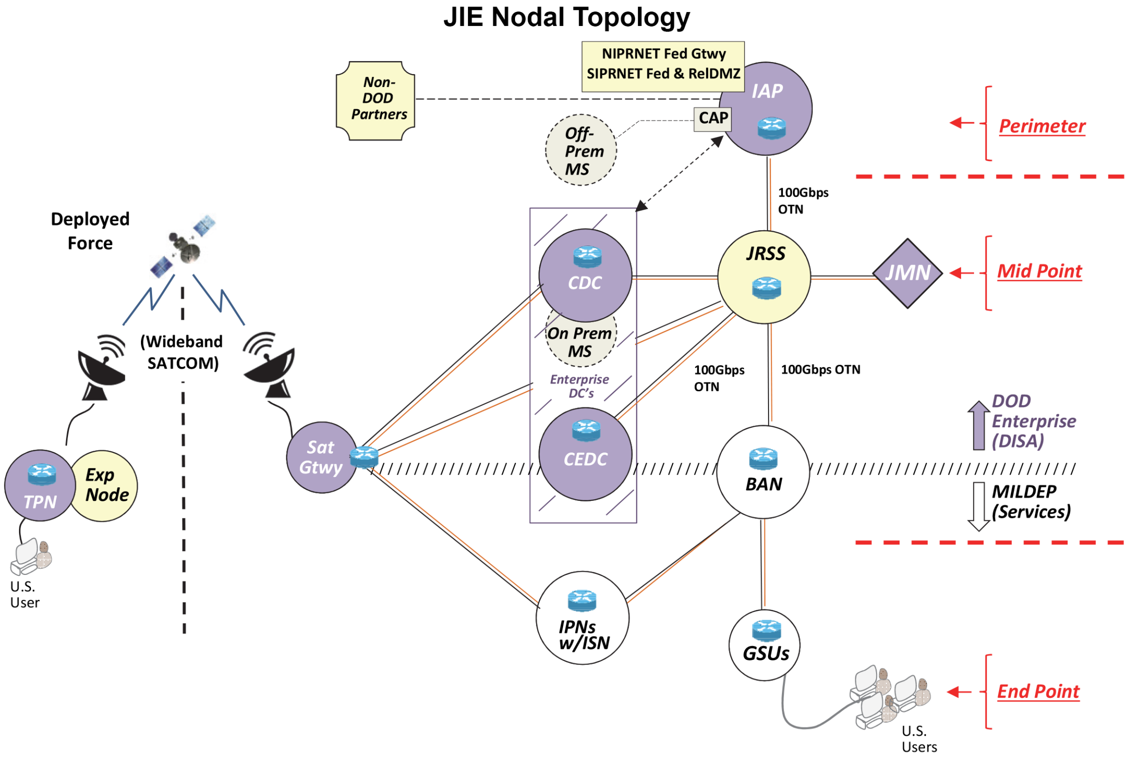
Joint Information Environment (JIE)

Executive Summary

- The Joint Information Environment (JIE) Executive Committee (EXCOM) continued to provide guidance and direct the implementation of the funded initiatives supporting the 10 JIE capability objectives and integration efforts for the DOD.
- The Deputy SECDEF designated the Secretary of the Air Force as the DOD Executive Agent for Mission Partner Environment (MPE) capabilities in February 2019.
- The Air Force conducted a programmatic and technical assessment of the MPE portfolio and assumed responsibility in FY19.
- The USD(A&S) approved the Defense Enterprise Office Solution (DEOS) contract award in August 2019, which went under protest in September 2019, and now has an anticipated contract award in January/February 2020. The DEOS program plans to use commercial cloud platforms to store classified and unclassified data.



BAN - Base Area Network
CAP - Cloud Access Point
CDC - Core Data Center
CEDC - Component Enterprise Data Center
DCs - Data Centers
DISA - Defense Information Systems Agency
DMZ - Demilitraized Zone
Exp - Expeditionary
Fed - Federal
Gbps - Gigabits per second
GSUs - Geographically Separated Unit

Gtwy - Gateway
IAP - Internet Access Point
IPNs - Installation Processing Node
ISN - Installation Service Node
JMN - Joint Management Network
JRSS - Joint Regional Security Stack
MILDEP - Military Department
MS - Materiel Solution
NIPRNET - Non-classified Internet Protocol Router Network

Off-Prem - Off premises
On-Prem - On premises
OTN - Optical Transport Network
Prem - Premises
RelDMZ - SIPRNET Releasable DMZ
Sat - Satellite
SATCOM - Satellite Communications
SIPRNET - Secret Internet Protocol Router Network
TPN - Tactical Processing Node

- In 2019, the DEOS Program Management Office (PMO) and the Joint Interoperability Test Command prepared the DEOS Phase 1 Test and Evaluation Master Plan (TEMP) that is in staff review for approval in FY20.
- DOT&E has stressed the need for DOD to conduct threat-representative cybersecurity testing on commercial cloud platforms to be used by DEOS.

Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE concept as a secure environment, comprising a single security architecture, shared information technology (IT) infrastructure, and enterprise services.
- The JCS intend JIE to consist of multiple subordinate programs, projects, and initiatives managed and implemented by the Defense Information Systems Agency (DISA) and the Military Services.
- In January 2017, the JIE EXCOM approved the following 10 JIE capability objectives:
  - Modernize Network Infrastructure, to include optical carrier upgrades, multi-protocol label switching, satellite communication gateway modernization, and Internet Protocol (IP) version 6 implementation
  - Enable Enterprise Network Operations, to include establishing global and regional operations centers, a JIE out-of-band management network, and converging IT service management solutions
  - Implement Regional Security, to include the Joint Regional Security Stack (JRSS), and the Joint Management System for JRSS
  - Provide MPE-Information System (IS) for coalition/partner information sharing, to include virtual data centers, services, and Mission Partner Gateways

- Optimize Data Center Infrastructure
- Implement Consistent Cybersecurity Architecture/ Protections, to include DOD enterprise perimeter protection, endpoint security, mobile endpoint security, data center security, cybersecurity situational awareness analytic capabilities, and identity and access management (referred to as the Single Security Architecture in older JIE documentation)
- Enhance Mobility for unclassified and classified capabilities
- Standardized IT Commodity Management, to include enterprise software agreements, license agreements, hardware agreements, and IT asset management
- Establish End-User Enterprise Services, to include the Enterprise Collaboration and Productivity Services (ECAPS) and converged voice and video services over IP
- Provide Hybrid Cloud Computing Environments, to include Commercial Cloud, Cloud Access Points, and milCloud

- The JCS envision JIE as a shared information technology construct for DOD to reduce costs, improve and standardize physical infrastructure, increase the use of enterprise services, improve IT effectiveness, and centralize the management of network defense. The Joint Staff specifies the following enabling characteristics for JIE capability objectives:
  - Transition to centralized data storage
  - Rapid delivery of integrated enterprise services (such as email and collaboration)
  - Real-time cybersecurity awareness
  - Scalability and flexibility to provide new services
  - Use of common standards and operational techniques
  - Transition to the JIE Cybersecurity Architecture
- JIE is not a program of record and does not have a traditional milestone decision authority, program executive organization, and project management structure that would normally be responsible for the cost, schedule, and operational performance of a program.
- The DOD Chief Information Officer (CIO) is the overall lead for JIE efforts with support from the JIE EXCOM – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6. The EXCOM provides JIE direction and objectives. DISA is the principal integrator for JIE capabilities and testing.

Activity

JIE

- For the JRSS version 1.5 operational assessment completed in July 2019, see the JRSS article on page 41.
- The JIE EXCOM continued to provide guidance and direct the implementation of the funded initiatives supporting the 10 JIE capability objectives and integration efforts for the DOD.
- The DOD CIO, Joint Staff, Combatant Commands, Services, and DOD Agencies continued efforts to collaboratively develop and build the JIE Cybersecurity Architecture.

ECAPS

- In 2019, the DEOS (ECAPS capability set 1) PMO and the Joint Interoperability Test Command prepared the DEOS Phase 1 TEMP that is in staff review for approval in FY20.
- In August 2019, the USD(A&S) approved the DEOS contract award, which then went under protest in September 2019, and now has an anticipated contract award in January/February 2020.
- DOT&E placed DEOS on the Operational Test Oversight List in September 2019.
- In coordination with the DOD CIO, the USD(A&S) is evaluating and refining the ECAPS capability sets 2 and 3 requirements through 2QFY20.

MPE

- The Deputy SECDEF designated the Secretary of the Air Force as the DOD Executive Agent for MPE and the DOD CIO as the Principal Staff Assistant for MPE in February 2019.
- The intent is to rationalize and modernize the overall MPE portfolio of command and control, and intelligence information sharing capabilities.
- The MPE-IS initiative is intended to consolidate and recapitalize 28 physical Combined Enterprise Regional Information Exchange Systems across the DOD, providing virtualized enduring and episodic MPE-IS services tailored to meet mission partner information sharing needs.
- The Air Force conducted a programmatic and technical assessment of the MPE portfolio and assumed responsibility in FY19.

Assessment

- The DOD CIO, DISA, and Services intend to achieve the JIE objectives through implementation of enabling initiatives aligned under the JIE EXCOM approved and funded priorities.
- The JIE EXCOM has started efforts to monitor JIE capability performance factors; however, the EXCOM does not place high enough priority on developmental and operational test results to inform decisions.
- The accelerated and compressed DEOS Phase 1 schedule is overly aggressive and high risk such that little time is factored in to find and resolve functional and cybersecurity problems before advancing to the next test and fielding event.
- Because the DEOS program plans to use commercial cloud platforms to store classified and unclassified data, it will be critical for 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 DEOS PMO has not planned or contracted for a DEOS integration lab to provide an operationally representative environment, so all DEOS developmental, cybersecurity, and operational testing will be conducted on production networks.

Recommendations

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

1. Conduct thorough cybersecurity operational testing of all JIE capabilities, including threat-representative testing of the commercial cloud capabilities employing current cybersecurity testing guidance and policy.
2. Use operational test information, such as that from the recent JRSS operational assessment, to inform JIE decisions.
3. Update the MPE-IS Test and Evaluation Strategy based on the Air Force programmatic and technical assessment.
4. Update the DEOS Phase 1 TEMP based on the contract award and update the master schedule.
5. Revise the DEOS schedule to make it supportable, resourced, and event-driven to guide both the capability development and the testing approach.
6. Establish an operationally representative DEOS integration lab for conducting developmental testing and initial cybersecurity assessments.
7. Develop the DEOS Phases 2, 3, and 4 TEMP Addenda to prepare stakeholders for the remaining deliveries, resource commitments, and T&E goals.
8. Develop a TEMP for ECAPS capability sets 2 and 3, and more generally for each JIE capability objective with funded initiatives.