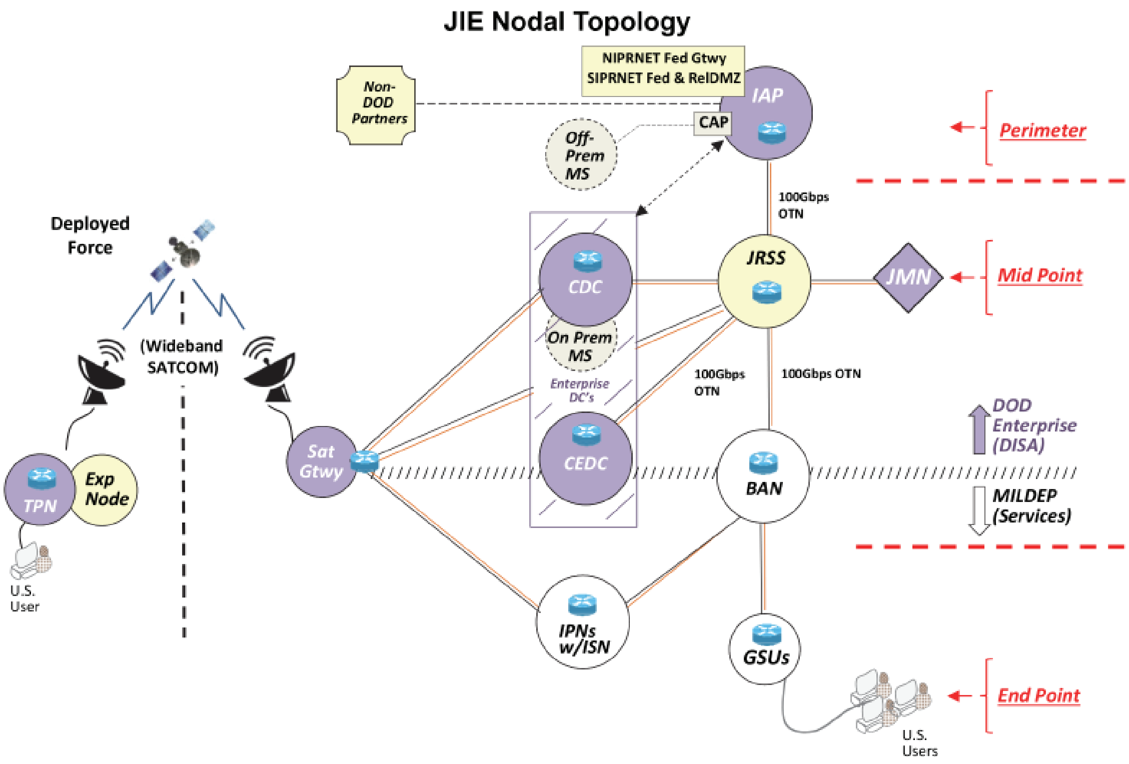
Joint Information Environment (JIE)



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

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 cybersecurity effectiveness of the Joint Regional Security Stack (JRSS), a component of JIE, calls into question the current JIE cybersecurity approach. For reporting on the JRSS, see the separate article on page 45.
- The USD(A&S) approved the Defense Enterprise Office Solution (DEOS) acquisition strategy in June 2018.
- The Deputy SECDEF intends to designate the Secretary of the Air Force as the DOD Executive Agent for Mission Partner Environment (MPE) capabilities in FY19.
- The Air Force is conducting a programmatic and technical assessment of the MPE portfolio and will assume responsibility in FY19.

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.
- JIE consists 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 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 (previously 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 envisions 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 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 reporting on the JRSS, see the separate article on page 45.
- 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 2018, the DEOS (ECAPS capability set 1) Program Management Office (PMO) and the Joint Interoperability Test Command began efforts to draft a DEOS Test and Evaluation Master Plan (TEMP).
- The USD(A&S) approved the DEOS acquisition strategy in June 2018, and, in coordination with the DOD CIO, is refining the ECAPS capability sets 2 and 3 requirements evaluation through 1QFY19.

MPE

- The Deputy SECDEF intends to designate 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 FY19.
  - 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 (CENTRIXS) across the DOD, providing virtualized enduring and episodic MPE-IS services tailored to meet mission partner information sharing needs.
  - The Air Force is conducting a programmatic and technical assessment of the MPE portfolio and will assume responsibility in FY19.

Assessment

- The DOD CIO, DISA, and Services intend to achieve the JIE goals through implementation of initiatives aligned under the JIE EXCOM-approved capability objectives.
- 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 cybersecurity effectiveness of the JRSS, a component of JIE, calls into question the current JIE cybersecurity approach.

Recommendations

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

1. Use operational test information, such as that from the recent JRSS operational assessments, to inform JIE decisions.
2. Update the MPE-IS Test and Evaluation Strategy upon completion of the Air Force programmatic and technical assessment.
3. Update the DEOS TEMP for approval once the PMO awards a contract and updates the master schedule.
4. Develop a Test and Evaluation Strategy for ECAPS and more generally for each JIE capability objective with funded initiatives.
5. Conduct thorough cybersecurity operational testing of all JIE capabilities, employing current cybersecurity testing guidance and policy.