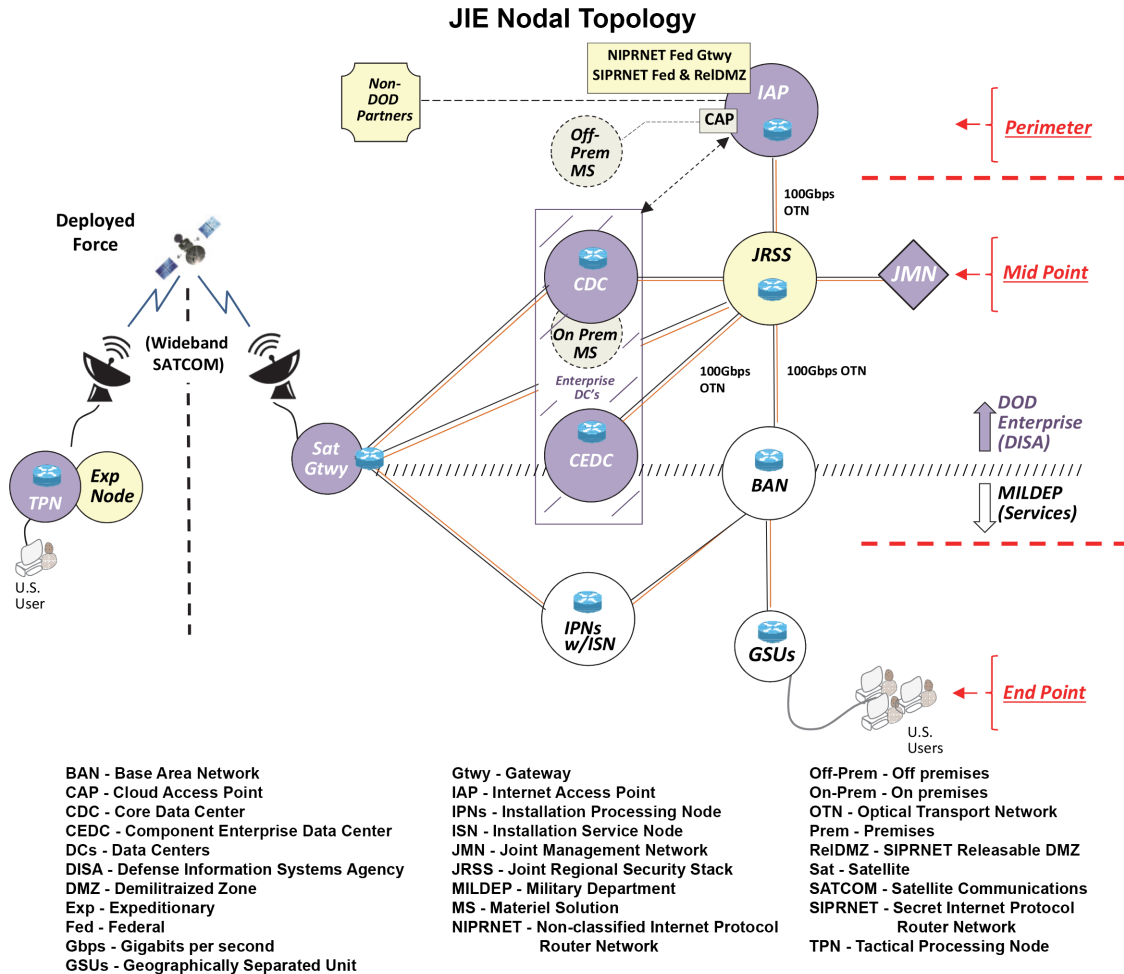


# Joint Information Environment (JIE)



## Executive Summary

- The Joint Information Environment (JIE) Executive Committee (EXCOM) approved 10 JIE capability objectives in January 2017 that prioritize JIE capability development and integration efforts for the DOD.
- DOT&E worked with the DOD Chief Information Officer (CIO) to develop a Mission Partner Environment – Information System (MPE-IS) Test and Evaluation Strategy in March 2017. MPE-IS integration, developmental testing, and rehearsals coincide with Exercises Steadfast Cobalt and Bold Quest 2017 to support and inform a DOD independent study report due in 2018.

## Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE concept as a secure environment, comprised of a single security architecture, shared information technology (IT) infrastructure, and enterprise services.

- JIE consists of multiple subordinate programs, projects, and initiatives managed by the Defense Information Systems Agency (DISA) and the Services.
- The DOD CIO established 10 JIE capability objectives that include the following:
  - 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 Stacks (JRSS), and the Joint Management System for JRSS

# FY17 DOD PROGRAMS

- Provide MPE-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 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 performance of a program.
- The DOD CIO leads 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 services and testing.

---

## Activity

- For reporting on the JRSS, see the separate article on page 69.
- The JIE EXCOM approved 10 JIE capability objectives in January 2017 that prioritize JIE capability development and integration efforts for the DOD.
- The DOD CIO developed an MPE-IS Test and Evaluation Strategy in March 2017. MPE-IS integration, developmental testing, and rehearsals coincide with Exercises Steadfast Cobalt and Bold Quest 2017 to support and inform a DOD-directed independent study for future funding in 2018.
- The JIE EXCOM approved the JIE Architecture and Engineering Security Classification Guide in May 2017, and the strategy document, Achieving the JIE Vision, in August 2017.
- The DOD CIO began development of a JIE Capabilities Test and Evaluation, and Assessment Concept whitepaper in June 2017.
- The JIE Capabilities Test and Evaluation Working Group is developing a JIE Test and Evaluation Strategy.
- The USD(AT&L) commenced acquisition strategy development for the Defense Enterprise Office Solution and the ECAPS components of JIE in February 2017.
- The DOD CIO, Joint Staff, Combatant Commands, Services, and DOD Agencies continued efforts to develop and build the JIE Cybersecurity Architecture.

## 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 priority on developmental and operational test information when making capability fielding decisions.
- The JIE EXCOM utilizes schedule-driven management but should adopt event-driven decision processes supported by developmental and operational test reporting.

## Recommendations

- Status of Previous Recommendations. The DOD CIO, JIE EXCOM, and Director of DISA satisfactorily addressed two of the previous non-JRSS specific FY16 recommendations. The following remain:
  1. Establish an overarching JIE program executive to integrate the system efforts and oversee cost, schedule, and performance.
  2. Complete, adopt, and implement the JIE Test and Evaluation Strategy.
- FY17 Recommendations. The DOD CIO, JIE EXCOM, and Director of DISA should:

## FY17 DOD PROGRAMS

1. Use operational test information to inform JIE capability fielding decisions.
2. Update the MPE-IS Test and Evaluation Strategy to reflect full delivery and test schedule upon completion of the independent study and DOD funding decision.
3. Develop a test and evaluation strategy for ECAPS and more generally for each JIE capability objective with funded initiatives.
4. Conduct thorough cybersecurity testing of JIE capabilities.

# FY17 DOD PROGRAMS