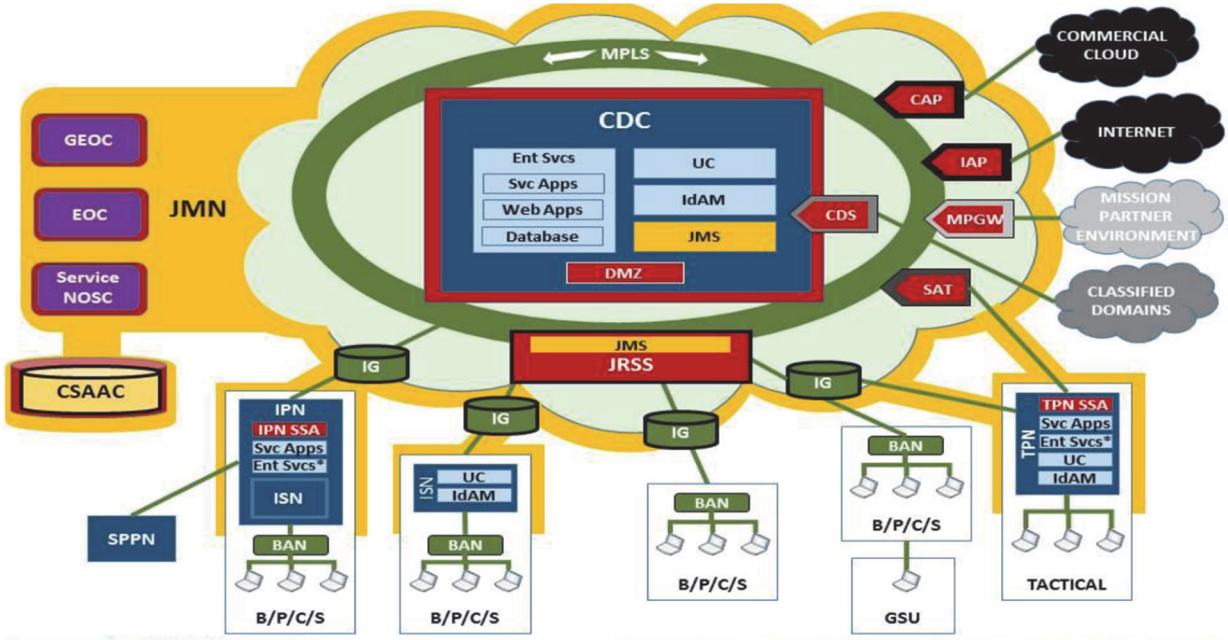
Joint Information Environment (JIE)



B/P/C/S - Base, Post, Camp, and Station
BAN - Base Area Network
CAP - Cloud Access Point
CDC - Core Data Center
CDS - Cross Domain Solution
CSAAC - Cyber Situational Awareness Analytic Cloud
Data Svcs - Data Services
DMZ - Demilitarized Zone
Ent Svcs - DOD Enterprise Services (*Extended)
EOC - Enterprise Operations Center
GEOC - Global Enterprise Operations Center
GSU - Geographic Separated Unit
IAP - Internet Access Point
IdAM - Identitiy and Access Managment
IG - Installation Gateway
IPN - Installation Processing Nodes
ISN - Installation Service Node
JMN - JIE Management Network
JMS - JIE Management System
JRSS - Joint Regional Security Stacks
MPGW - Mission Partner Gateway
MPLS - Multiprotocol Label Switching
NOSC - Network Operations & Security Center
SAT - Satellite Communications Gateway
SPPN - Special Purpose Processing Node
SSA - Single Security Architecture
Svc Apps - DOD Component Applications
TPN - Tactical Processing Node
UC - Unified Capabilities
Web Apps - Web Applications

Executive Summary

- The Joint Information Environment (JIE) is not a program of record, and to date, the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), and Services have not conducted any operational testing of the JIE infrastructure or components.
- The JIE effort lacks an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors. The European JIE early operational assessment, originally scheduled for March/April 2014, continues to slip due to Joint Regional Security Stack (JRSS) integration complexity, lack of overall schedule discipline, and Service-influenced funding priorities; the DOD Chief Information Officer (CIO) has shifted its near-term focus for JRSS to the Southern Continental United States (CONUS).
- U.S. Cyber Command established the Joint Force Headquarters DOD Information Networks (JDOC) and the JIE Executive Committee (EXCOM) designated the DISA Operation Centers in Europe and the Pacific as Enterprise Operations Centers (EOCs) to support JIE network management, data centers, Internet gateways, JRSS, and cybersecurity. The Joint Operations Steering Group (JOSG) developed EOC continuity of operations plans to better manage networks, and coordinate and communicate with Service operations centers. DISA established EOCs in the European and Pacific theaters that will conduct mission support and information technology operations.
- DOT&E is working with DISA and JITC to plan for an early operational assessment of JIE in late FY16.
- U.S. Cyber Command continues to refine the selection criteria for the CONUS EOCs as well as the JDOC/EOC global and regional situational awareness requirements. In October 2015, the JIE EXCOM endorsed U.S. Cyber Command's proposal that DISA CONUS be the interim EOC to support the implementation of JRSS.

Capability and Attributes

- The DOD CIO has prioritized areas of modernization for the DOD components to implement as the foundational steps to realize the JIE. The DOD CIO's areas of modernization include the following:

  - Network Modernization of optical carrier upgrades and Multi-Protocol Label Switching (MPLS) routers
  - The JRSS, the Joint Management System for the JRSS and Cyber Situational Awareness Capabilities
  - Computing Environment, which includes Commercial Cloud, Cloud Access Points, and milCloud
  - The Mission Partner Environment for coalition/partner information sharing and the Mission Partner Gateways
  - Mobility for the unclassified and classified capabilities
- The JIE is envisioned as a shared information technology construct for DOD to reduce costs, improve and standardize physical infrastructure, increase the use of enterprise services, improve information technology effectiveness, and centralize the management of network security. The Joint Staff specifies the following enabling characteristics for the JIE capability:
  - 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 a single security architecture
- The DOD plans to achieve these goals via the following interrelated initiatives:
  - Consolidation of applications and data into the cloud or centralized data centers at the regional or global level, which are not segregated by military Service.
  - Establishment of enterprise operation centers to centralize network management and defense.
  - Upgrade of the physical infrastructure to include MPLS, which enables higher bandwidth/throughput, better security, and faster routing capabilities.
  - Implementation of JRSS hardware and other security constructs as part of a single security architecture. These will establish a federated network structure with standardized identity and access management, as well as centralized defensive cyber operations.
- JIE is not a program of record, but is being governed by the DOD CIO, with DISA as the principal integrator for services and testing. An EXCOM, chaired by the DOD CIO, U.S. Cyber Command, and the Joint Staff J6, provides JIE direction, goals and objectives, oversight, and accountability.
- The initial implementation of the JIE is underway in the United States and in the European theater with the establishment of the first JRSS capabilities, JDOC and EOCs, and the European data centers. Installations are ongoing in Europe with tentative implementation and cutover dates in June/July 2016. Additional preparation efforts are ongoing in the Pacific, Southwest Asia, and CONUS.

Activity

- The JIE EXCOM rescheduled an early operational assessment of the European theater capabilities originally planned for March 2014 to 4QFY16 or later to accommodate the engineering, installation, and implementation of the initial JRSS and MPLS capabilities. The DOD CIO has shifted its near-term focus for JRSS to the Southern CONUS.
- JITC developed an evaluation framework that maps testable JIE metrics back to the requirements and high level objectives.
- U.S. Cyber Command established the JDOC and the JIE EXCOM designated the DISA Operation Centers in Europe and the Pacific as EOCs to support JIE network management, data centers, Internet gateways, JRSS, and cybersecurity.
- The JOSG developed EOC continuity of operations plans to better manage networks, and coordinate and communicate with Service operations centers.
- DISA established EOCs in the European and Pacific theaters that will conduct mission support and information technology operations.
- In May and July 2015, the Army, Air Force, DISA, and JITC conducted JRSS lab-based tests at Fort Meade, Maryland, and Joint Base San Antonio, Texas.
- Developmental and laboratory testing continues at initial JRSS sites at Fort Hood and Joint Base San Antonio, Texas, and the DISA Enterprise Services Lab at Fort Meade, Maryland. Current testing focuses on system functionality; however, a Cyber Protection Team (CPT) conducted a hunt mission to find outstanding vulnerabilities in the operational management network and the Joint Base San Antonio JRSS from March to May 2015.
- In October 2015, the JIE EXCOM approved the JIE high-level objectives and initial performance metrics.
- U.S. Cyber Command continues to refine the selection criteria for the CONUS EOCs as well as the JDOC/EOC global and regional situational awareness requirements. In October 2015, the JIE EXCOM endorsed U.S. Cyber Command's proposal that DISA CONUS be the interim EOC to support the implementation of JRSS.
- DOT&E, USD(AT&L), DOD CIO, the Services, DISA, and JITC repurposed the JIE T&E working-level Integrated Product Team into an overarching working group to better synchronize the test preparations and ongoing activities.
- A CPT and the Army's Advanced Research Lab conducted a comprehensive vulnerability and penetration assessment against the JRSS in the Fort Meade labs in 4QFY15.
- JITC conducted the JRSS version 1.0 Initial Operational Assessment with a Red Team to assess Army and Air Force operations in December 2015.

Assessment

- The JIE is not a program of record, and to date, DISA, JITC, and Services have not conducted any operational testing of the JIE infrastructure or components.
- The DOD CIO is the lead for JIE governance; however, the JIE effort lacks an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors. The European JIE early operational assessment continues to slip due to JRSS integration complexity, lack of overall schedule discipline, and Service-influenced funding priorities. While the near-term focus for JRSS has shifted to the Southern CONUS, advanced planning for future capability deployment and operational tests has not fully matured.
- No operational test data are available at this point.
- Current testing focuses on system functionality; DISA has yet to schedule full cybersecurity testing or operational testing of the JRSS.
- DOT&E is working with DISA and JITC to plan for an early operational assessment of JIE in late FY16.
- DISA and JITC scheduled a lab-based Computer Network Defense Exercise for mid-October 2015 but it was delayed due to other assessment activities. The National Security Agency plans to conduct a cybersecurity deep-dive assessment in FY16.

Recommendations

- Status of Previous Recommendations. The DOD CIO and Director of DISA continue to address the previous FY14 recommendations to develop adequate test schedules and plans for anticipated future test events in FY16.
- FY15 Recommendations. The DOD CIO, JIE EXCOM, and DISA should:
  1. Establish an overarching JIE program executive to integrate the system efforts and oversee cost, schedule, and performance.
  2. Consider managing the key JIE capabilities/components with program managers.
  3. Continue to develop an overarching test strategy that encompasses not only the upcoming testing of JIE, but also defines the key issues and concepts to be tested in subsequent tests and assessments. Such a plan should address the following areas of interest:
     - Overarching T&E framework and critical test issues
     - The role of both lab and fielded equipment tests in resolving those critical issues
     - Estimated schedules for test events and key issues to be tested
     - Evaluation criteria and any relevant implementation decision points
     - Resources required
     - The role of the Services and Service-sponsored Operational Test Agencies