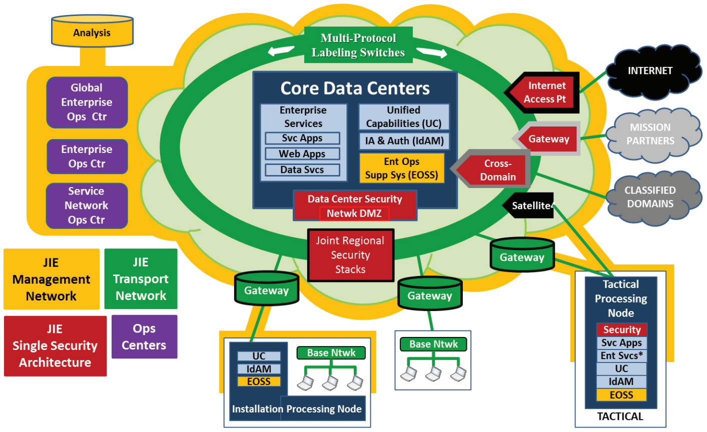
Joint Information Environment (JIE)

Executive Summary

- Following the establishment of requirements by a Chairman of the Joint Chiefs of Staff White Paper and Deputy Secretary of Defense implementation guidance in 2013, DOT&E placed the Joint Information Environment (JIE) on test and evaluation oversight in August 2013.
- JIE is not a program of record, and to date, the Defense Information Systems Agency (DISA) and the Services have not conducted any operational testing of the JIE infrastructure or components. Furthermore, the operational parameters required for DOT&E to review and evaluate JIE are still under development by U.S. Cyber Command.
- DOT&E is working with the DISA Test and Evaluation Office to plan for an early operational assessment of JIE in FY15.

Capability and Attributes

- The JIE is envisioned as a shared information technology construct for DOD to improve physical infrastructure, increase the use of enterprise services, 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)
  - Real-time cyber 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:
  - Implementation of Joint Regional Security Stack (JRSS) hardware and other security constructs as part of a single security architecture. These will establish a federated network structure with standardized access and authentication management, as well as centralized defensive cyber operations and DOD Information Network defense.
  - Consolidation of applications and data into centralized data centers at the regional or global level, which are not segregated by military Service.
  - Upgrade of the physical infrastructure to include Multi-Protocol Label Switching (MPLS), which enables higher bandwidth/throughput, and faster routing capabilities.
  - Establishment of enterprise operation centers to centralize network management and defense.
- JIE is not a program of record, but is being managed by the DOD Chief Information Officer (CIO), with DISA as the principal integrator for services and testing. An Executive Committee, chaired by the CIO, U.S. Cyber Command, and the Joint Staff J6, provide JIE governance. The initial implementation of the JIE has begun both in the U.S. and in the European theater with the establishment of the first capabilities. Installations are ongoing in Europe, but implementation and cutover dates remain uncertain. Additional theaters of interest are the Pacific, Southwest Asia, and the continental United States.



Base Ntwk - Base Network
Data Svcs - Data Services
EOSS - Ent Ops Supp Sys - Enterprise Operations Support System
Ent Svcs - Enterprise Services
IdAM - IA & Auth - Information Assurance and Authentication
Netwk DMZ - Network Demilitarized Zone
Ops - Operations
Ops Ctr - Operations Center
Svc Apps - Service Applications
UC - Unified Capabilities
Web Apps - Web Applications

Activity

- The Chairman, Joint Chiefs of Staff published a White Paper on the JIE in January 2013 and the Deputy Secretary of Defense published implementation guidance for JIE in May 2013. DOT&E subsequently put the JIE initiative on test and evaluation oversight in August 2013.
- DISA has rescheduled an early operational assessment of the European theater capabilities originally planned for March 2014 to 2QFY15 to accommodate the engineering, installation, and implementation of the initial JRSS and MPLS capabilities. DISA reports that these operational capabilities will be only partially implemented in time for the first operational assessment; DOT&E plans to conduct an additional assessment when the full capabilities are implemented. The availability of test sites for JIE and component tests are limited and advanced planning for future tests is not fully matured.
- In FY14, DISA conducted extensive lab-based testing and installation/functional testing of both JRSS and MPLS at the DISA facilities at Fort Meade, Maryland, and Joint Base San Antonio, Texas. While installations of key JIE infrastructure continue in the European area, training and

development of operational procedures and concepts are ongoing. The JRSS installation at Joint Base San Antonio is now providing some services to support both Army and Air Force network operations, but has not been fully implemented as yet. No operational tests have been conducted of JIE infrastructure, components, tactics, procedures, or operational concepts to date, but DOT&E continues to monitor the development of key test plans and concepts.
- DISA has established a test and evaluation working-level Integrated Product Team in which DOT&E, the Services, USD(AT&L), and DOD CIO representatives participate.

Assessment

- No operational test data are available at this point.
- Developmental and laboratory testing continues at initial JRSS sites at Joint Base San Antonio, Texas, and the DISA Enterprise Services Lab at Fort Meade, Maryland. To date, testing focuses on system functionality and DISA has not yet scheduled full cybersecurity testing.

Recommendations

- Status of Previous Recommendations. The DOD CIO and Director of DISA are addressing the previous recommendations in that test schedules and plans continue to be prepared for anticipated test events in FY15 and long-range and overarching test strategies are being developed.
- FY14 Recommendations. DISA should:
  1. Examine the availability of cyber range resources to augment the existing physical installations available for testing.
  2. Continue to develop an overarching test strategy that encompasses not only the upcoming testing of JIE in Europe, 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 decisions points
     - Resources required
     - The role of the Services and Service-sponsored Operational Test Agencies