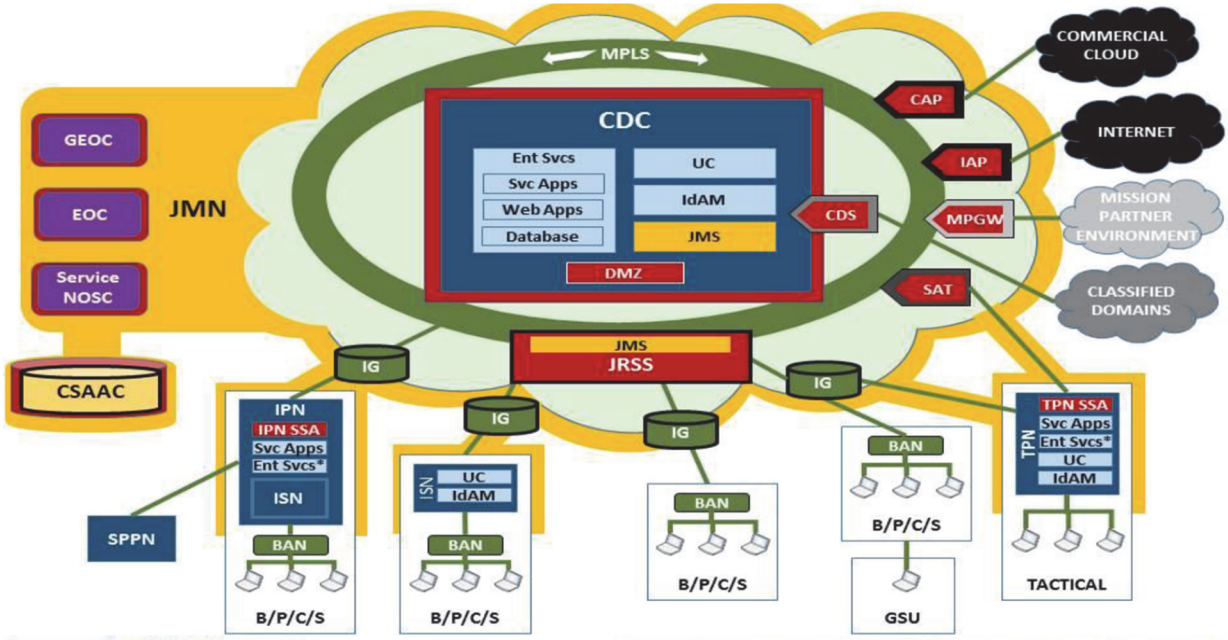
Joint Information Environment (JIE)



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

- Although the Joint Information Environment (JIE) is not a program of record, numerous programs, including but not limited to the Joint Regional Security Stack (JRSS), are directly associated with JIE, are expending significant and substantial resources, and are meant to execute critical missions. To date, the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), and Services have not conducted rigorous and comprehensive operational testing of any of the programs associated with JIE.
- The JIE Test and Evaluation Working Group, supported by DOT&E, the DOD Chief Information Officer (CIO), U.S. Cyber Command, and the Joint Staff J6 is developing a JIE test and evaluation strategy to assess the maturity of JIE capabilities through a series of annual operational assessments and an overarching operational test and evaluation, starting in July 2017.
- JIE efforts continue to lack an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors.
- DISA and the Services are pursuing a non-traditional acquisition approach for the JRSS that has led to early Army and Air Force fielding decisions uninformed by rigorous and comprehensive operational tests, despite the results of developmental tests and limited-in-scope operational assessments indicating JRSS users are not able to provide effective network security. Given the preeminent role that JRSS, once fielded, necessarily plays in securing the Department's networks, this early fielding of JRSS under circumstances in which users seem unable to employ it to secure their networks may unnecessarily jeopardize the security of critical DOD networks and systems.
- DOT&E and JITC planned for an operational assessment in December 2016 on the JRSSs fielded by the Air Force, but in late November 2016 the Air Force elected to postpone the assessment because of known problems with JRSS technology, training, and enterprise management and operator procedures, which severely limit the current cybersecurity effectiveness of the already fielded JRSS installations. Specifically, the 24th Air Force Commander was concerned that DOT&E might issue a report that reflected poorly on JRSS.
- In response to the DOT&E memos on JIE/JRSS signed in August and September 2016, the DOD CIO agreed that an

IOT&E event for JRSS will take place in May 2017, but this date will likely be revised based on the Air Force deferral of testing.

Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE as a secure environment, comprised of shared information technology (IT) infrastructure, enterprise services, and single security architecture.
- JIE consists of multiple subordinate programs, projects, and initiatives managed by DISA and the Services.
- The DOD CIO has prioritized areas of modernization of the DOD Information Network (DODIN) for DOD components to implement as the foundation for JIE. The DOD CIO's areas of modernization include the following:
  - Optical carrier upgrades and Multi-Protocol Label Switching (MPLS)
  - JRSS, the Joint Management System for JRSS, and Cyber Situational Awareness Capabilities
  - The Computing Environment, which includes Commercial Cloud, Cloud Access Points, and milCloud
  - The Mission Partner Environment-Information System, for coalition/partner information sharing, and the Mission Partner Gateways
  - Mobility for unclassified and classified capabilities
- 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 security. The Joint Staff specifies the following enabling characteristics for 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 CIO, DISA, and Services plan to achieve the JIE goals via the following interrelated initiatives:
  - Consolidate applications and data into the cloud or into centralized regional or global data centers that are not segregated by military Service.
  - Establish enterprise operation centers to centralize network management and defense.
  - Upgrade the network infrastructure to include MPLS routers and optical transport upgrades, which enhances network resiliency and bandwidth capacity, and improves security.
  - Implement JRSS architecture and other security constructs as part of a single security architecture. This will reduce the number of access points to the DODIN, standardize identity and access management, and enable centralized defensive cyber operations.
- 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. Moreover, an Operational Test Agency has not conducted independent operational testing required of a traditional acquisition program of record.
- The DOD CIO generally leads JIE efforts with support from the JIE Executive Committee (EXCOM) – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6 – which provides JIE direction, objectives, and limited accountability. DISA is the principal integrator for JIE services and testing.

Activity

- DISA and the Services continued implementation of key JIE enabling capabilities in the United States and in the European theater with the establishment of additional JRSS and MPLS capabilities.
  - JITC conducted an assessment of the JRSS version 1.0 with a Red Team to evaluate Army JRSS operations in December 2015 and published a test report in April 2016.
  - JITC conducted lab-based JRSS developmental testing and operational rehearsals during 2016.
  - In August 2016, the Air Force conducted an evaluation of JRSS with the objective of informing an Air Force JRSS operational trial period entry decision in September 2016. The Air Force decided to migrate three sites behind JRSS for operational trials, starting in October 2016, with plans to accelerate migration efforts in January 2017.
- The General Accountability Office published its JIE report in July 2016.
- In August and September 2016, DOT&E published three JIE/JRSS memos to the Services recommending that they conduct operational testing to ensure that the fielding decision authorities have full understanding of the capabilities and limitations that JRSS will provide before deciding to migrate to JRSS and depend upon it to protect their networks.
- DOT&E and JITC planned for an operational assessment in December 2016 on the JRSSs fielded by the Air Force, but in late November 2016 the Air Force elected to postpone the assessment because of known problems with JRSS technology, training, and enterprise management and operator procedures, which severely limit the current cybersecurity effectiveness of the already fielded JRSS installations. Specifically, the 24th Air Force Commander was concerned that DOT&E might issue a report that reflected poorly on JRSS.
- In response to the DOT&E memos on JIE/JRSS signed in August and September 2016, the DOD CIO issued a memo

in September 2016 agreeing that an IOT&E event for JRSS will take place in May 2017, but this date will likely be revised based on the Air Force deferral of testing. The DOD CIO memo also said that final JRSS migrations will not occur until operational testing satisfies the Military Services' requirements.
- The IOT&E event planned for May 2017 will inform Air Force leadership decisions to fully decommission legacy capabilities. Until full decommissioning occurs, it would be relatively easy to switch from JRSS back to legacy capabilities, if the Air Force chose to do so.
- The JIE Test and Evaluation Working Group, supported by DOT&E, the DOD CIO, U.S. Cyber Command, and the Joint Staff J6 is developing a JIE test and evaluation strategy.
- In August 2016, U.S. Cyber Command initiated an effort to develop a strategic direction for leveraging JRSS capabilities in support of their secure, operate, and defend the DODIN mission.

Assessment
- Although JIE is not a program of record, numerous programs, including but not limited to JRSS, are directly associated with JIE, are expending significant and substantial resources, and are meant to execute critical missions. To date, DISA, JITC, and the Services have not conducted rigorous and comprehensive operational testing of any of the programs associated with JIE.
- DISA and the Services are pursuing a non-traditional acquisition approach for the JRSS that has led to early Army and Air Force fielding decisions uninformed by rigorous and comprehensive operational tests, despite the results of developmental tests and limited-in-scope operational assessments indicating JRSS users are not able to provide effective network security. Given the preeminent role that JRSS, once fielded, necessarily plays in securing the Department's networks, this early fielding of JRSS under circumstances in which users seem unable to employ it to secure their networks may unnecessarily jeopardize the security of critical DOD networks and systems.
- Acquiring and deploying JRSS without operational testing significantly increases risks to the missions and forces which rely on the affected networks. The limited early test data reported by JITC in April 2016 shows that JRSS capabilities are immature, lacking a stable configuration, and that operator training is incomplete and insufficient. Of most concern is JITC's finding that key JRSS cybersecurity functions are not mission capable.
- Testers identified over three dozen deficiencies, including many scored as Category 1 Emergency and Category 1 Urgent priority problems.
  - Substandard JRSS capability performance areas included system scalability; reliable connectivity to JRSS components over the network; the absence of standardized tactics, techniques, and procedures; and inadequate operator proficiency, training, and documentation.
  - These problems affected critical capabilities and adversely affect the operational effectiveness of defensive cybersecurity operations.
  - Network traffic during the test traversed in series on both the JRSS and the existing Air Force gateway security stacks, with each stack potentially interfering with and affecting the function of the other security stack.
- Despite these test results, the Air Force plans to start fielding the JRSS to 14 bases between October and December 2016; the Army and Navy are also fielding, but at a slower pace.
- Fielding JRSS prior to verifying through rigorous operational testing and regressions that the technology works, and that JRSS operators and enterprise network defenders have effective procedures and training required to operate the system, risks degrading DOD network operations and security, potentially leaving networks vulnerable to undetected adversarial actions during and after JRSS migration.
- The DOD CIO is the lead for JIE governance; however, the JIE effort continues to lack an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors.

Recommendations
- Status of Previous Recommendations. The DOD CIO and Director of DISA have not addressed the previous FY14 and FY15 recommendations to:
  1. Develop adequate test schedules and plans for anticipated future test events in FY17 and beyond.
  2. Establish an overarching JIE program executive to integrate the system efforts and oversee cost, schedule, and performance.
  3. Manage all key JIE capabilities/components with empowered, responsible program managers.
  4. 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.
- FY16 Recommendations.
  1. To prevent unnecessary risks to DOD networks, the Services should stop fielding JRSS capabilities until the results of a comprehensive IOT&E show that the enterprise and Service operators are capable of using the JRSS to provide effective network security.
  2. Poor program governance and acquisition oversight for JRSS is jeopardizing the security of DOD networks; to address these issues Congress should consider directing the DOD to make JRSS an Acquisition Category IAM program of record.

  The DOD CIO, JIE EXCOM, and DISA should:
  3. Complete, adopt, and implement the JIE test and evaluation strategy.
  4. Conduct a JRSS IOT&E to evaluate JRSS capabilities, operator training, and enterprise processes and use the results to inform JRSS capability-related fielding and migration decisions.