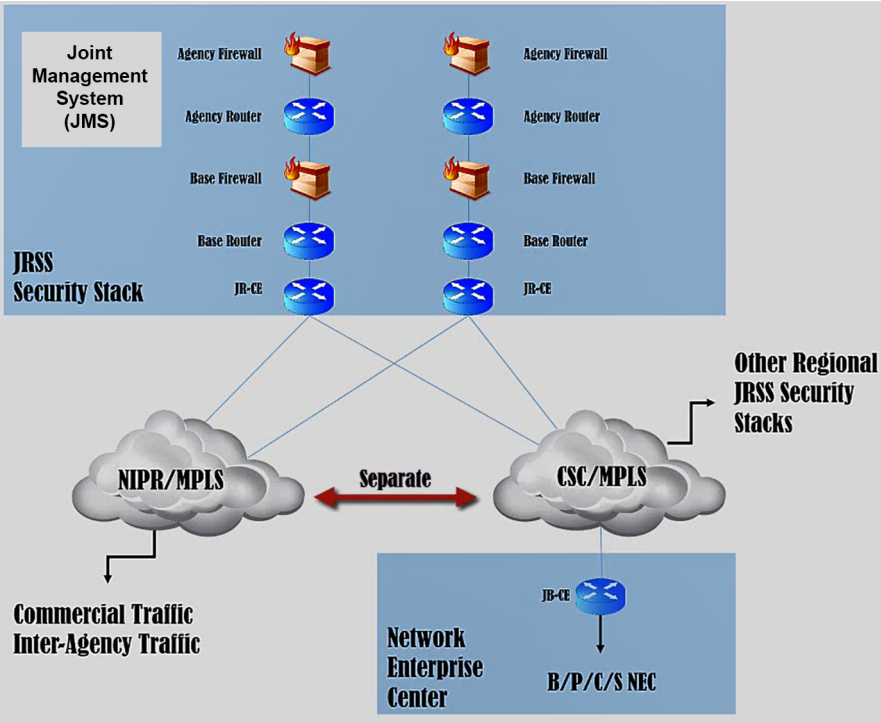
Joint Regional Security Stack (JRSS)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) of the NIPRNET-Joint Regional Security Stack (JRSS) (N-JRSS) in July 2019, in accordance with a DOT&E-approved test plan. The Air Force, Army, Navy, Coast Guard, and the Defense Information Systems Agency (DISA) Global participated in the event. Preliminary results show that JRSS continues to perform poorly against operationally realistic cyber-attacks on DOD networks.
- Migrations to use N-JRSS have continued and are not contingent upon operational test results, but the DOD Chief Information Officer (CIO) and the JRSS Program Manager (PM) use test results to track problems with the fielded system. Thirteen JRSSs are currently operational on the NIPRNET with 20 total planned for fielding.
- Operator proficiency is a persistent shortfall identified by operational testing, indicating the JRSS training processes and system usability need improvement.
- Despite the above, the DOD plans to deploy JRSS on the DOD classified SIPRNET. DOT&E is working with the JRSS PM and the DOD CIO to plan cybersecurity assessment activity to inform the SIPRNET-JRSS (S-JRSS) trial migration decisions scheduled in FY20. This effort will also help develop and validate S-JRSS joint operator tactics, techniques, and procedures (TTPs), which are currently in development. The PM plans to field a total of 25 S-JRSSs.



B/P/C/S - Base, Post, Camp, Station
CSC - Carrier Supporting Carrier
JB-CE - Joint Base - Customer Edge
JR-CE - Joint Router- Customer Edge
JRSS - Joint Regional Security Stack
MPLS - Multi-Protocol Label Switching
NEC - Network Enterprise Center
NIPR - Non-classified Internet Protocol Router Network

Capabilities and Attributes

- As a component of the Joint Information Environment (JIE), JRSS is a suite of equipment intended to perform firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding, as well as to provide a host of network security capabilities. JRSS is not a program of record. Despite its complexity, the DOD has treated JRSS as a "technology refresh," and has not funded the personnel and training typically associated with DOD acquisition programs of record.
- The JRSS is intended to centralize and standardize network security into regional architectures instead of locally distributed, non-standardized architectures at different levels of maturity and different stages in their lifecycle at each military base, post, camp, or station.
- Each JRSS includes many racks of equipment designed to allow DOD components to ingest, process, and analyze very large network data flows.
- The DOD intends to deploy JRSS on both the NIPRNET (N-JRSS) and SIPRNET (S-JRSS).
- DISA is the designated approving and certification authority for both JRSS equipment and multiprotocol label switching (MPLS) equipment. MPLS is part of a modernization effort to upgrade the bandwidth capacity of the Defense Information Systems Network.
- A key component of JRSS is the Joint Management System (JMS), which provides centralized management of cybersecurity services required for DOD Information Network (DODIN) operations and defensive cyber operations.

Mission

The DOD intends to use JRSS to enable DOD cyber defenders to continuously monitor and analyze the DODIN for increased situational awareness to minimize the effects of cyber-attacks while ensuring the integrity, availability, confidentiality, and non-repudiation of data.

Vendors

DISA is the lead integrator for JRSS. The tables below list the current Original Equipment Manufacturers (OEMs) of the JRSS capabilities.

OEM	OEM Location
A10	San Jose, California
Argus	Houston, Texas
Axway	Phoenix, Arizona
Bivio	Pleasanton, California
BMC	Houston, Texas
Bro	Berkeley, California
Cisco	San Jose, California
Citrix	Fort Lauderdale, Florida
CSG International	Alexandria, Virginia
Dell	Round Rock, Texas
EMC	Santa Clara, California
F5	Seattle, Washington
Fidelis	Bethesda, Maryland
Gigamon	Santa Clara, California
HP	Palo Alto, California
IBM	Armonk, New York
InfoVista	Ashburn, Virginia
InQuest	Arlington, Virginia
Juniper	Sunnyvale, California

OEM	OEM Location
Micro Focus	Rockville, Maryland
Microsoft	Redmond, Washington
Niksun	Princeton, New Jersey
OPSWAT	San Francisco, California
Palo Alto	Santa Clara, California
Quest	Aliso Viejo, California
Raritan	Somerset, New Jersey
Red Hat	Raleigh, North Carolina
Red Seal	Sunnyvale, California
Riverbed	San Francisco, California
Safenet	Belcamp, Maryland
Splunk	San Francisco, California
Symantec	Mountain View, California
Trend Micro	Irving, Texas
Van Dyke	Albuquerque, New Mexico
Veeam	Columbus, Ohio
Veritas	Mountain View, California
VMWare	Palo Alto, California

Activity

- Because of problems found with fielded N-JRSS during operationally realistic testing, in 2018, the JIE Executive Committee directed a JRSS Strategic Review and subsequent actions to address shortfalls in training, migration, system performance, JRSS on SIPRNET, and operational processes. These actions concluded in early CY19.
- In December 2018, the JRSS Senior Advisory Group (SAG) requested that the DOD CIO staff and the JRSS PM conduct one-on-one meetings with each Service to ascertain their problem priorities for correction. The PM continues to work corrective actions for the problems identified by the Services.
- JITC conducted a JRSS Operations Rehearsal (OR) in January/February 2019. JITC had planned the event as an OA, but de-scoped the assessment to a rehearsal after the planned Red Team became unavailable. The JRSS OR focused on 10 open problem reports from previous events. JITC assessed that four problems had been corrected and discovered two new problems.
- In March 2019, the JRSS SAG directed JITC to propose updated Measures of Performance to be used in the July 2019 OA, which the SAG endorsed in early July 2019.
- In March 2019, a Red Team began aggressing Service networks protected by JRSS to establish network presence over the course of 4 months.
- In July/August 2019, the JRSS PM and JITC conducted an OA on N-JRSS as a risk reduction event in accordance with a DOT&E-approved test plan to assess Air Force, Army, and Navy JRSS instantiations and to validate resolution of a subset of problem reports identified during previous tests. Of the 17 problem reports assessed, 8 were closed, 9 remain open, and 5 new reports were created. The Coast Guard participated, but was not evaluated.
- In October 2019, the JRSS PM and the DOD CIO, in collaboration with DOT&E, began planning cybersecurity assessment activity to inform S-JRSS trial migration decisions in FY20, and to inform the development of S-JRSS joint TTPs.

Assessment

- Analysis of the July/August 2019 OA is ongoing. JITC conducts OAs every 6 months in a schedule-driven approach that does not allow sufficient time to report on findings, correct problems, and update test plans.
- Preliminary OA results indicated that JRSS continues to perform poorly against operationally realistic cyber-attacks on DOD networks.

- The OA provided useful Service user feedback:
  - Some test scenarios did not accurately represent the various ways in which different Services use the JRSS.
  - New users wanted better training to understand how JRSS should be configured and used to support their missions. The OA revealed that user training continues to be insufficient, as Service users had gaps in their knowledge of various JRSS tools.
  - Service users do not have good insight into the status of their trouble tickets or the ticket resolution process.
- The extended Red Team activity, executed in support of the OA, was more limited in duration and scope than a Persistent Cyber Opposing Force assessment, but provided an informative prototype for future instantiations of such an effort.
- The JRSS PM and DOD CIO are engaging in efforts to improve current JRSS configurations, training, and procedures, and to migrate new users to N-JRSS and S-JRSS. Testing has enabled the JRSS PM to identify improvements and correct problems with the fielded system. However, capability deployment and user migrations are not contingent upon proven performance in operationally realistic testing.
- JITC has not conducted a Cooperative Vulnerability and Penetration Assessment or Adversarial Assessment on JRSS components or their associated management networks. These assessments are necessary to resolve the cybersecurity posture of the stacks themselves. JITC is planning to conduct these assessments for the first time on N-JRSS in FY20.
- Outside of operational test events, routine cyber assessments on networks protected by JRSSs, such as using a threat-representative Persistent Cyber Opposing Force, are not being conducted. Doing so would help program efforts to discover and address critical cyber vulnerabilities, and provide continual feedback on JRSS network defense effectiveness against operationally realistic cyber-attacks.
- JRSS test requirements derive from a Functional Requirements Document that the DOD CIO and U.S. Cyber Command (USCYBERCOM) have not updated as operational needs and funding priorities have evolved. JITC has also not updated the JRSS Test and Evaluation Strategy to reflect changing priorities.
- The JRSS PM and DOD CIO have not initiated a Validated Online Lifecycle Threat (VOLT) assessment analysis with the Defense Intelligence Agency (DIA) in accordance with DOD policy. Doing so would support PMO assessments of capability gaps against likely threat capabilities.
- The results of the 1QFY20 pre-migration cybersecurity assessment of S-JRSS will provide critical entrance criteria to the formal migration decisions.

Recommendations

- The DOD CIO and the DOD Components should:
  1. Discontinue migrating new users to JRSSs until the system demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks.
  2. Prioritize training, system usability, and operator proficiency over meeting migration schedule deadlines.
  3. Engage with USCYBERCOM and Joint Force Headquarters (JFHQ)-DODIN to establish a process to regularly update the Functional Requirements Document to reflect Service requirements, funding availability, and project capability needs identified by the mission owners.
  4. Engage with USCYBERCOM and JFHQ-DODIN to produce an operational requirements document.
  5. Coordinate with JITC to update the JRSS Test and Evaluation Strategy to support capability implementation and DOD Component requirements.
- The JRSS PM, DISA Global, and the DOD Components should:
  1. Use operationally realistic test results to improve current JRSS configurations, training, and procedures, and to inform future N-JRSS and S-JRSS migration decisions.
  2. Address any new problems discovered during the recent July/August 2019 OA and from previous testing.
  3. Formalize and promulgate a joint problem reporting and tracking system for problems discovered in both tests and in real-world operations to allow user visibility and cross-Component situational awareness into the status of known unresolved and resolved problems.
- DISA and the DOD Components should:
  1. Verify JRSS operator competency and training to properly configure and use JRSS services prior to new user migrations.
  2. Engage with JFHQ-DODIN to include JRSS in upcoming Persistent Cyber Opposing Force efforts to routinely discover and address critical cyber vulnerabilities on operational networks.
- DISA (JRSS PM), DOD Components, and JITC should:
  1. Conduct a review of the test scenarios and measures to ensure that each Components' unique testing needs are met and that inconsistencies between test scenarios and DOD Components' actual procedures are minimized.
  2. Plan to conduct Cooperative Vulnerability and Penetration Assessments and Adversarial Assessments of the N-JRSS and S-JRSS stacks and their associated management networks.
- DISA (JRSS PM) should:
  1. Engage with DIA for a VOLT analysis, which can be used to inform the Adversarial Assessment efforts planned for FY20 and beyond.