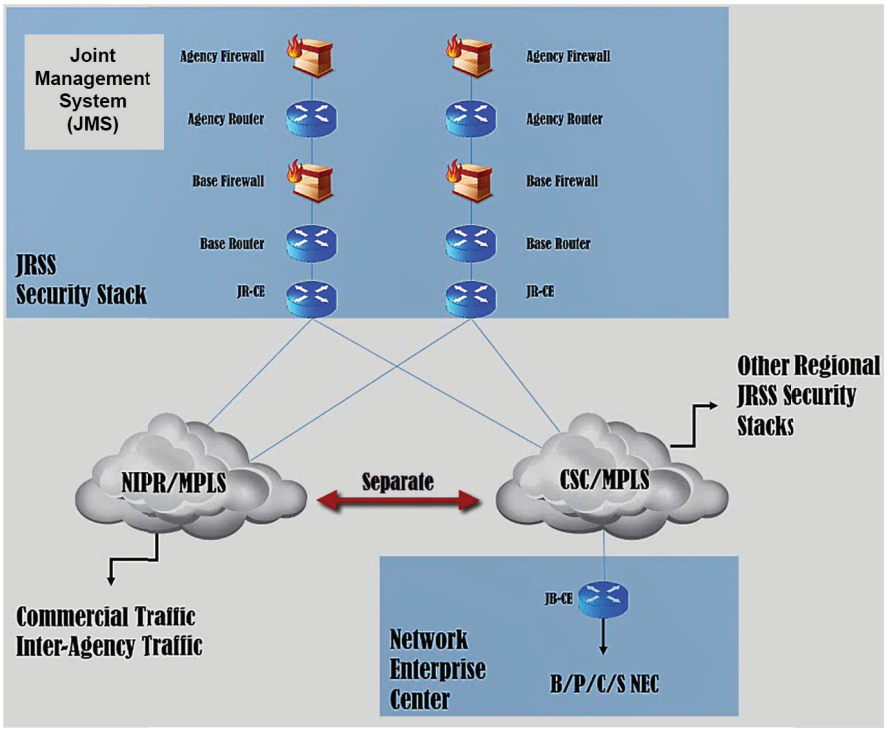
Joint Regional Security Stack (JRSS)

Executive Summary

- In March 2018, the Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) that demonstrated that the Joint Regional Security Stack (JRSS) Version 1.5, as utilized by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. The JRSS showed little improvement from the OA conducted in July 2017.
- The following factors affected the OA results: 1) the difficulty inherent in integrating disparate, complex commercial technologies into a functional system of systems; 2) although improving, training remains insufficient, and; 3) standard operating procedures (SOPs) remain immature.
- Since the OA, JRSS has continued to experience operational and technical problems, including high latency that adversely impacted the Joint Service Provider, Army Materiel Command (AMC) and U.S. Southern Command (SOUTHCOM) and delayed migration of additional users associated with those components.
- Over the last 2 years, the JRSS Program Manager has continued to address persistent problems with JRSS; however, it remains unclear whether the very high volume of data designed to traverse each JRSS can be managed effectively.
- Due to the poor JRSS performance, the JRSS Senior Advisory Group (SAG) and Executive Committee for Joint Information Environment (JIE EXCOM) delayed the JRSS migration for U.S. Central Command, Southwest Asia (Army), and the Marine Corps, and deferred JRSS deployments for SIPRNET until FY19.
- On May 10, 2018, the JIE EXCOM conducted a Strategic Review of JRSS. The JIE EXCOM approved an adjustment to migration schedules and redirected resources to mitigate JRSS performance, training, and operational process issues based on testing results and operational lessons learned. Operational assessments are scheduled for January and July 2019, and every 6 months until the IOT&E, tentatively scheduled for FY20
- On June 28, 2018, the JIE EXCOM approved the proposed timeline to implement actions across these lines of effort: training, migration, capability, JRSS deployments for SIPRNET, and operational governance. Efforts are ongoing by the JRSS Program Manager and stakeholders to correct findings from previous test events, with status reports provided monthly to the JIE EXCOM.



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

- Defense Information Systems Agency (DISA) Global Operations Command reported that they require 17 additional government positions (e.g., engineers, administrators, development operations manager, and project managers) at DISA, Global Operations Command East (DGOC-E) to cover manning shortfalls with plans to be properly manned by July 2019.
- The Army (Regional Cyber Center-Continental United States) could not certify that they had sufficient manning to assume the JRSS mission.
- Fourteen JRSSs are currently deployed on the NIPRNET, (23 are planned). No JRSSs are currently deployed on SIPRNET (25 are planned).

Capabilities and Attributes

- As a component of the 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 provide a host of network security capabilities. Neither JIE nor JRSS is a program 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, which allow DOD components to intake, process, and analyze very large network data flows.
- The Services and DISA intended 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 (DISN). DISA will implement MPLS/JRSS-enabling technology to increase network speed and manage the larger traffic flows.
- A key component of JRSS is the Joint Management System (JMS) that provides centralized management of cybersecurity services required for DOD Information Network (DODIN) operations and defensive cyber operations.

Mission

DISA and the Services intend 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 threats while ensuring the integrity, availability, confidentiality, and non-repudiation of data.

Vendors

DISA is the lead integrator for JRSS. The tables below lists 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

- JITC conducted an OA of the JRSS Version 1.5 in March 2018.
- On May 10, 2018, the JIE EXCOM approved an adjustment to migration schedules and redirected resources to mitigate JRSS performance, training, and operational process issues based on testing results and operational lessons learned.
- On June 28, 2018, the JIE EXCOM approved the JRSS Strategic Review, which delayed N-JRSS migrations and deferred S-JRSS migrations until FY19. The program manager and stakeholders have undertaken efforts to correct findings from previous test events and make improvements along five lines of effort: training, migration, capability, S-JRSS, and governance.
- In August 2018, JITC hosted a 5-day JRSS Lab-based Exercise (LBE) to prepare the Army, Air Force, and Navy for the planned 2019 operational testing, to facilitate hands-on learning for other Services prior to their migration behind JRSS, and to provide an opportunity for DOD components to

exercise their SOPs. Thirteen components participated in the LBE and several others observed.

Assessment

- The March 2018 OA demonstrated that the JRSS, as the Joint Regional Security Stack (JRSS) Version 1.5, as utilized by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. JRSS performed poorly, and showed little improvement from the July 2017 OA. JRSS operators did not detect the Air Force 177th Information Aggressor Squadron as it portrayed a cyber adversary attacking the Enclave Control Node logically situated behind JRSS defenses. The following shortfalls contributed to poor JRSS cybersecurity performance:
  - It is inherently difficult to effectively manage the very large amount of data designed to traverse each JRSS.
  - Although the JRSS uses commercial off-the-shelf technologies, JRSS operator training still lags behind JRSS deployment, and is not sufficient to prepare operators to effectively integrate and configure the complex suite of JRSS hardware and associated software.
  - The Services, DISA, and U.S. Cyber Command have not codified JRSS joint tactics, techniques, and procedures to ensure unity of defensive effort and enhance defensive operations.
  - DISA Global and the Army have insufficient manning to properly operate JRSS.

Recommendations

1. The DOD Chief Information Officer (CIO) and the Services should discontinue deploying JRSSs until the system demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks.
2. The JRSS Program Manager, DISA Global, and the Services should:
   - Use operationally realistic test results to improve current JRSS configurations, training, and procedures, and to inform future N-JRSS and S-JRSS migration decisions
   - Address problems discovered during the most recent OA and from previous testing before proceeding to other tests
   - Include the Army, Navy, and Marine Corps JRSS configurations in future operational tests
3. The DOD CIO and the Services should consider the possibility that the data flow designed to traverse each JRSS may be too large to enable secure data management, and if that is the case, refine the JRSS deployment plans to reduce the required data flow through each JRSS.
4. DISA and the Services should ensure sufficient trained personnel are available to support JRSS migration schedules.
5. DISA and the Services should conduct routine cyber assessments of deployed JRSSs, using a threat representative Persistent Cyber Opposing Force, to discover and address critical cyber vulnerabilities.