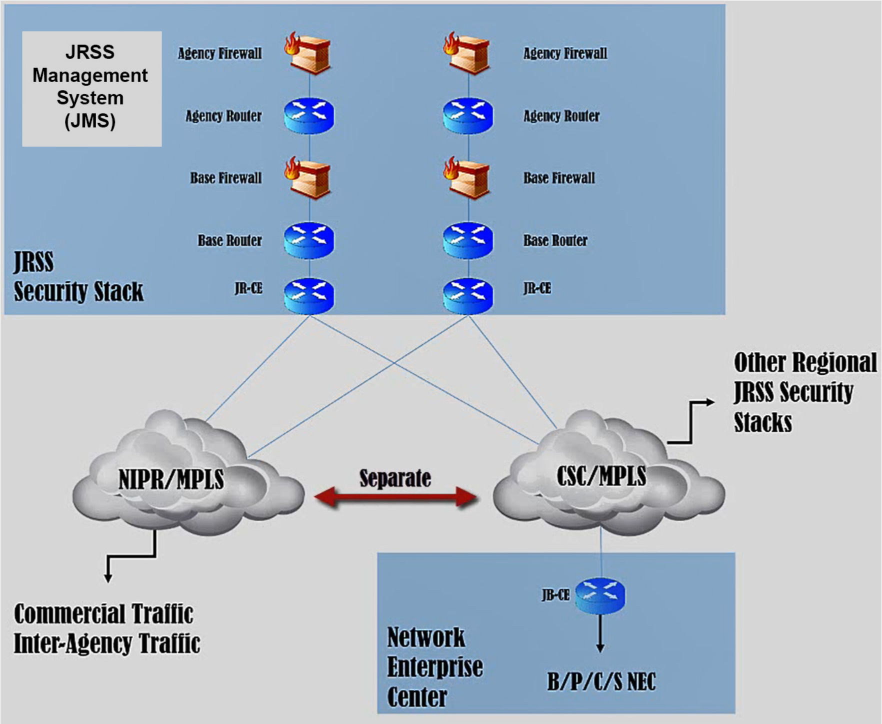
Joint Regional Security Stack (JRSS)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) that demonstrated that the Joint Regional Security Stack (JRSS) Version 1.5, as fielded by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. This is because integration of the disparate commercial technologies is complex and the JRSS training and standard operating processes are not yet mature enough to take advantage of the capabilities offered by the equipment.
- In accordance with DOD Chief Information Officer (CIO) guidance, the Army, Air Force, and other DOD components continue to deploy JRSS to operational DOD networks, despite testing that demonstrates JRSS technology integration, training, and Service and agency processes are not able to protect networks from cyber-attacks.
- The Air Force JRSS operators state that JRSSs are undermanned; Defense Information Systems Agency (DISA) Global is staffed for four stacks but manages nine, and the Air Force is at 50 percent manning for JRSS. DISA and the Services need to ensure that fielding and JRSS training are synchronized to overcome shortfalls.
- The Senior Advisory Group (SAG) for JRSS wisely delayed the IOT&E until 2QFY19 to assure test adequacy and Red Team availability for the cybersecurity Adversarial Assessment.



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

Capability 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 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 racks of equipment, which allow DOD components to intake, process, and analyze large sets of network data.
- The Services and DISA intended to deploy JRSS on both the Non-classified Internet Protocol Router Network (NIPRNET (N-JRSS)) and SECRET Internet Protocol Router Network (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 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.

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
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
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

- DISA and JITC conducted an OA of N-JRSS version 1.5 in July 2017 in accordance with a DOT&E-approved test plan.
- Also in July 2017, the DOD CIO approved and signed the JRSS Test and Evaluation Strategy version 1.14.
- In August 2017, U.S. Cyber Command (USCYBERCOM) signed the JRSS Concept of Operations, which provides the foundational concepts and operational framework for the integration and synchronization of joint Cyberspace Operations that leverage JRSS.
- The JIE Executive Committee approved the "JRSS Operations Training Requirements Document" in April 2017; the purpose of the document is to codify training requirements that will "lead to a future JIE state of enterprise training standardization."
- In September 2017, the JRSS SAG deferred the JRSS IOT&E to 2QFY19 with the following conditions:
  - Conduct another OA of N-JRSS version 1.5 in 2QFY18 to establish N-JRSS version 1.5 operational performance, after addressing the shortfalls discovered during the July 2017 OA.
  - Conduct an OA of N-JRSS version 2.0 in 1QFY19 that will include participants from the Army, Air Force, Navy, DISA Global, and potentially other DOD components.
- The JRSS SAG deferred the IOT&E for the following reasons:
  - To alleviate a test adequacy concern: not all planned traffic (email) would have traversed JRSS during the IOT&E because the Air Force would not have retired the associated Gateways. One of the purposes of the IOT&E is to help inform the Air Force of the risk of retiring all of their legacy Gateways, which currently provide some cybersecurity capability.
  - Lack of available cyber Red Teams to conduct the test.
  - A USCYBERCOM scheduled Period of Non-Disruption, which would have prevented a failover test.
  - To provide time for the Services and DISA to mitigate problems identified in the OA.

Assessment

- The OA demonstrated that the JRSS, as fielded by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. This is because integration of the disparate commercial technologies is complex and the JRSS training and standard operating processes are not yet mature. The following shortfalls contributed to poor JRSS cybersecurity performance:
  - Although the JRSS uses mature, commercial-off-the-shelf technologies, JRSS operator training lags behind JRSS deployment, and is not sufficient to prepare operators to

effectively integrate and configure the complex, room-sized suite of JRSS hardware and associated software.

- The Services, DISA, and USCYBERCOM have not codified JRSS joint tactics, techniques, and procedures to ensure unity of defensive effort and enhance defensive operations.
- Air Force JRSS operators state that JRSSs are undermanned; DISA Global is staffed for four stacks but manages nine, and the Air Force is at 50 percent manning for JRSS.

- DOT&E intends to publish a classified report on the OA results in January 2018.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations.

1. The CIO and the Services should discontinue deploying JRSS until the JRSS demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks.
2. Because of the lack of trained personnel, DISA and the Services should conduct training and deployment analysis to ensure sufficient trained personnel are available to meet fielding schedules.
3. The JRSS Program Office should use operationally realistic testing results to improve current JRSS configurations, training, procedures, and inform future JRSS fielding decisions.
4. The JRSS Program Office should work closely with JITC to schedule and fund adequate FOT&E of future incremental versions of both N-JRSS and S-JRSS.
5. DISA and the Services should conduct periodic cyber assessments of the JRSS, using a threat representative Persistent Cyber Opposing Force, to discover and address critical cyber vulnerabilities.