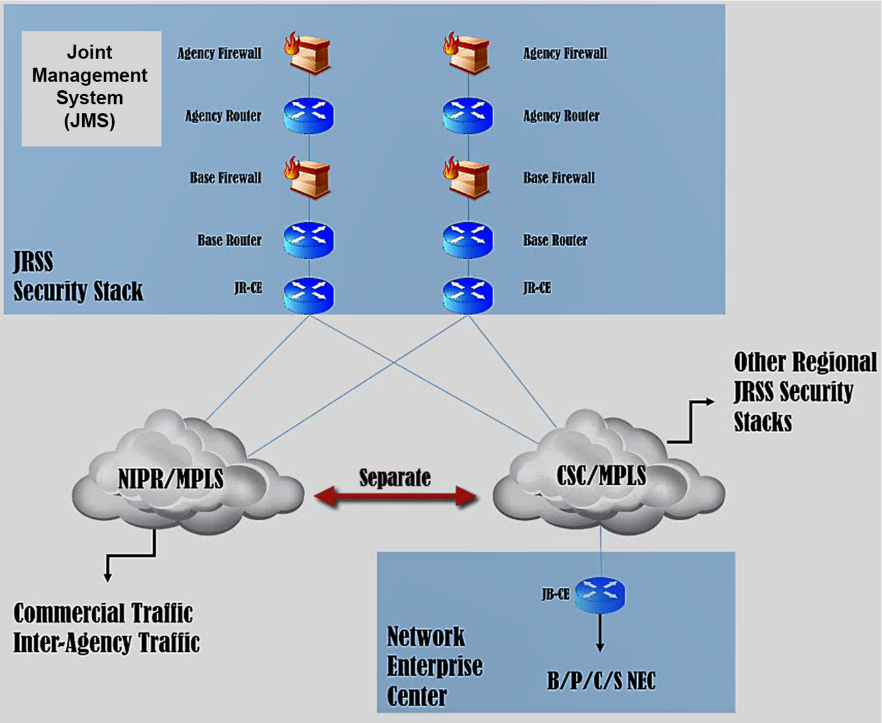
Joint Regional Security Stack (JRSS)

Executive Summary

- In February 2020, the DOT&E Advanced Cyber Operations (ACO) team and the Defense Information Systems Agency (DISA) Red Team, in coordination with the Joint Regional Security Stack (JRSS) Program Management Office (PMO), conducted a cyber event. This event was to evaluate the cyber posture of SIPRNET-JRSS (S-JRSS), the SIPRNET Joint Management Network (S-JMN), and the SIPRNET-Joint Management System (S-JMS). The event resulted in poor cybersecurity findings, which contributed to the PMO shutting down existing S-JRSSs and the Digital Modernization Infrastructure Executive Committee (DMI EXCOM) delaying future S-JRSS deployments to FY23.
- Proven, effective cybersecurity performance in operationally realistic testing has not been a criterion for NIPRNET (N-JRSS) fielding. Since 2016, N-JRSS operational assessments have continually shown that N-JRSS is unable to help network defenders protect DOD Component networks against operationally realistic cyberattacks.
- U.S. Cyber Command (USCC), with DOT&E assessment support, is helping the Services pilot implementation of Zero Trust architectures as the DOD evaluates a more data-centric security model. This new model promises more effective cybersecurity than the perimeter defenses currently offered by JRSS.

Capabilities and Attributes

- 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.



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

- 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.
- JRSS is currently operational on NIPRNET (N-JRSS). A SIPRNET (S-JRSS) version was planned with several being installed, but not used operationally, in 2016.

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 cyberattacks while ensuring the confidentiality, integrity, availability, and non-repudiation of data.

Vendors

DISA is the lead integrator for JRSS. The table on the next page lists the current Original Equipment Manufacturers (OEMs) of the JRSS capabilities.

OEM	OEM Location
A10	San Jose, California
Axway	Phoenix, Arizona
BMC	Houston, Texas
Bro	Berkeley, California
Cisco	San Jose, California
Citrix	Fort Lauderdale, Florida
Corelight	San Franciso, California
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
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
Zeek (formerly Bro)	Berkeley, California

Activity

- JRSS is not a program of record and does not have a Test and Evaluation Master Plan (TEMP).
- In December 2019, the PMO conducted an N-JRSS Tools Rationalization meeting where representatives of the JRSS operational community met to discuss how the portfolio of tools available in JRSS are used with the goal to identify redundant and/or unused capabilities.
- In February 2020, DOT&E and the DISA Red Team, in collaboration with the PMO, examined the cybersecurity of four deployed S-JRSS stacks that did not yet have operational traffic flowing, the S-JMN, and the S-JMS.
- The Joint Interoperability Test Command (JITC) planned a cooperative vulnerability and penetration assessment (CVPA) of N-JRSS for February 2020. This event was postponed due to delays in funding and travel authorizations for critical support personnel. JITC rescheduled the event in July 2020 but could not conduct it due to coronavirus (COVID-19) pandemic travel restrictions.
- JITC is currently planning a fully remote CVPA in October 2020 to work around travel restrictions.
- In January-March 2020, the JRSS PMO conducted a pilot implementation of a Break and Inspect (B&I) capability for selected encrypted traffic outbound to the internet on two N-JRSS production stacks within the continental United States (CONUS).
- In April 2020, the DOD Chief Information Officer (CIO) published an update to the JRSS Functional Requirements Document, in response to a DOD Inspector General recommendation to map the test measures to requirements. JRSS does not have documented operational requirements.
- In June 2020, the Air Force stopped funding their 346th Test Squadron's support of JRSS testing.
- In August 2020, the DMI EXCOM (formerly Joint Information Environment EXCOM) approved a reduced spending plan for FY22 which defers S-JRSS efforts to FY23. In the interim, the DOD will consider alternative mid-tier defensive cybersecurity solutions.
- In September 2020, DOT&E began a series of validation events to support the cybersecurity evaluation of USCC Zero Trust pilots being executed by the Services.

Assessment

- Migrations to N-JRSS are not contingent upon operational test results and have continued despite DOT&E recommendations to suspend them until the stacks are shown to be effective in operational testing. Since 2016, N-JRSS operational assessments have continually shown that N-JRSS is unable to help network defenders protect DOD Component networks against operationally realistic cyberattacks.
- A report from the December 2019 N-JRSS Tools Rationalization meeting has not yet been released to external participants. Appropriate and effective Standard Operating Procedures (SOP) and training for JRSS network defense operations have still not been developed.
- The February 2020 cybersecurity event for S-JRSS, the S-JMN, and the J-JMS produced poor cybersecurity findings

that contributed to the decision to shut down the existing S-JRSS stacks and delay full deployment. Users had not yet migrated behind the existing stacks deployed in 2016.

- The PMO's N-JRSS B&I pilot focused on network performance and degradation, and showed minimum performance effect during high bandwidth availability in CONUS only.
  - No tests were conducted to determine latency affects over long haul communications, or on latency sensitive applications and tactical edge platforms.
  - The pilot did not evaluate cybersecurity risks of the B&I capability or if it can contribute to effective cyber defense, which are critical factors in adopting the capability.
  - Furthermore, the DOD Components requested that the B&I capability provides visibility into traffic that traverses within the DODIN vice internet bound traffic. This pilot only collected data on the latter.
  - In September 2020, the JRSS Senior Advisory Group voted to put implementation of JRSS B&I on hold until further analysis of the capability, and how it should be used across the DOD, is conducted.
- JITC has been unable to conduct test events in 2020 initially due to delays in funding and travel authorizations, and then due to COVID-19-related travel restrictions. JITC has shifted focus to conducting remote testing where possible, with the support of the DOD CIO and the PMO.
- Although the DOD CIO has mapped test measures to functional requirements, an operational requirements document still does not exist. In order to fully address users' and mission owners' needs during testing, operational requirements must be documented.
- Because JRSS is already deployed, and to minimize the need to travel, the DOD CIO, the JRSS PMO, JITC, and DOT&E are working to streamline JRSS evaluation by taking better advantage of existing operational data elements and focusing test events on the risks associated with system changes intended to improve mission effectiveness.
- Given the effect of COVID-19, user migrations and testing schedules are curtailed, presenting an opportunity to focus on operator training and streamlining the JRSS capabilities to improve user experience and mission effectiveness. Operator proficiency is a persistent shortfall identified by operational testing, indicating the JRSS training processes and system usability need improvement.
- The Air Force decision to stop supporting the 346th Test Squadron's participation in JRSS testing caused testers to lose insight into the Air Force's methods, priorities, and topology making evaluation of the Air Force's JRSS use less effective.
- The DOD is evaluating the adoption of a data-centric security model over the traditional network-centric security for the Department. The results of the USCC Zero Trust pilots, which DOT&E is helping assess for cybersecurity through a series of validation events, will be used to guide future directions for mid-tier security. In advance of DOD migrating users to Zero Trust environments, often enabled through software-defined perimeter capabilities, the concept, design, and use of N-JRSS will need to be revised to effectively and suitably support and integrate into the defensive cyber mission.

Recommendations

- The DOD CIO and the DOD Components should:
  1. Continue developing more effective cybersecurity alternatives to JRSS, such as the ongoing pilot work by the Services on implementing Zero Trust architectures and increased focus on developing and maintaining a skilled and trained defensive cyber work force.
  2. Should forgo S-JRSS operations altogether if the Zero Trust architectures prove viable.
  3. 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 cyberattacks and until the mid-tier cybersecurity analyses from USCC, DOD CIO, the DOD Principal Cyber Advisor, and external consultants inform future directions.
  4. Reevaluate the need for an N-JRSS B&I functional requirement as USCC and DOD CIO analyze how to best use and implement traffic inspection capabilities within the DODIN.
  5. Prioritize training, system usability, and operator proficiency over meeting migration schedule deadlines.
  6. Engage with USCC and Joint Force Headquarters-DODIN to establish a process to regularly update the Functional Requirements Document to reflect Service requirements, funding availability, and the evolving capability needs identified by the mission owners.
  7. Produce an operational requirements document to improve the N-JRSS defense against nation state threats.
- The JRSS PMO, DISA Global, and the DOD Components should:
  1. Continue focus on training and SOP development. Operator training is an important factor for mission success, and recent minimum staffing changes as part of the COVID-19 response make operator competency more important.
- 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.
- DISA (JRSS PMO), DOD Components, and JITC should:
  1. Coordinate with the Service cyber commands and operational community to identify real-world testing metrics and data sources to support remote evaluation and supplement operational test data.
- The Air Force should:
  1. Consider restoring funding for JRSS testing to the 346th Test Squadron to represent Air Force interests and knowledge in test planning, test conduct, and real-world operational data collection and analysis for continued JRSS performance evaluation.