# Joint Regional Security Stack (JRSS)

Previous assessments demonstrated that the Joint Regional Security Stack (JRSS) was not effective in helping cyber defenders detect and respond to operationally realistic cyber threats. Pursuant to the FY21 National Defense Authorization Act (NDAA), in July 2021, the DOD Chief Information Officer (CIO) decided not to deploy JRSS on SIPRNET and sunset NIPRNET JRSS within the next five years while pursuing a Zero Trust cybersecurity architecture.

## System Description

JRSS is a suite of cybersecurity capabilities intended to protect the Department of Defense Information Network (DODIN). The DOD intends to use JRSS to enable DOD cyber defenders to continuously monitor and analyze DODIN traffic to minimize the effects of cyberattacks while ensuring the integrity, availability, confidentiality, and non-repudiation of data. The suite of capabilities integrated as part of JRSS are to support both defensive cyber operations and network operations for bases, posts, camps, and stations.

## Program

JRSS is not a program of record and does not have a Test and Evaluation Master Plan. The Defense Information Systems Agency (DISA) manages the technical implementation of JRSS, while the DOD CIO chairs the JRSS Senior Advisory Group (SAG) that governs programmatic aspects of the system. The Services jointly fund JRSS and manage their own use of its capabilities. JRSS is currently operational on NIPRNET. A SIPRNET version was planned, with several being installed in 2016, but not used operationally. Pursuant to the 2021 NDAA, the DOD CIO elected to sunset JRSS within five years rather than transition it to a program of record.

### Major Contractors

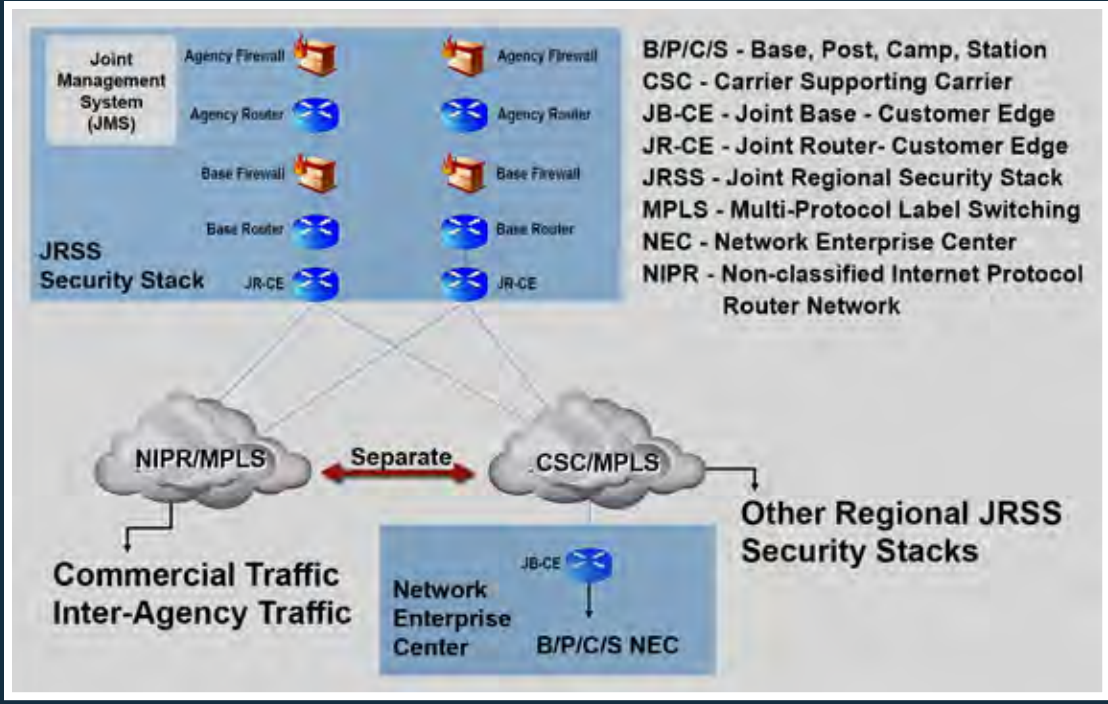
DISA is the lead integrator for JRSS. The paragraph below lists the current Original Equipment Manufacturers (OEMs) of the JRSS capabilities.

- A10 – San Jose, California.
- Ansible – Durham, North Carolina.
- Axway – Phoenix, Arizona.
- BMC – Houston, Texas.
- Cisco – San Jose, California.

- Citrix – Fort Lauderdale, Florida.
- Corelight (Zeek) – San Francisco, California.
- Confluent (Kafka) – Mountain View, California.
- CSG International – Alexandria, Virginia.
- Dell – Round Rock, Texas.
- Elastic – Mountain View, California.
- 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.
- ITIPIE – Springfield, 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.

## Test Adequacy

In September 2020, the JRSS SAG implemented an updated test strategy that relies on the Joint Interoperability Test Command (JITC) to continuously monitor the live system and produce risk assessments of new capabilities to determine the necessary level of test. These monitoring and risk assessment processes are still maturing, causing new challenges for JITC and the test community. JRSS upgrade schedules have not been made available to assist in planning risk assessments, and the JRSS Program Management Office (PMO) has not committed to considering operational test data in deployment or migration decisions. JITC is also working to identify




**Joint Regional Security Stack (JRSS)**

additional measures to include in their continuous monitoring reports.

In October 2020, JITC and the Army Combat Capabilities Development Command Data and Analysis Center conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) of selected JRSS stacks. This event was adequate to inform the PMO of findings to help improve system security, but did not support a decision.

# Performance

## Effectiveness

Previous operational assessments of JRSS have demonstrated that JRSS capabilities do not help cyber defenders thwart operationally realistic cyber threats. No operational test events were conducted in 2021 that provided data on JRSS operational effectiveness.

## Suitability

Previous operational assessments of JRSS have shown that operator proficiency is a persistent shortfall, indicating the JRSS training processes and system usability need improvement. JITC has produced two quarterly reports on some aspects of JRSS for the continuous monitoring approach, which have not indicated problems with stack availability. No operational test events were conducted in 2021 that provided data on JRSS operational suitability.

## Survivability

The October 2020 CVPA yielded findings that the PMO could use to improve system security. A follow-on Adversarial Assessment has not yet occurred due to Red Team availability and the pending migration to System Integration and Event Management (SIEM) 2.0.

# Recommendations

1. The DOD CIO and the DOD Components should transition from JRSS to a Zero Trust cybersecurity architecture, involving layered and data-centric security as quickly as possible.
2. The JRSS PMO should generate, maintain, and make available a master schedule, which shows the final capability developments currently anticipated, as well as major strategic milestones for sun-setting JRSS. The schedule should be reconciled with progress and milestones for the incoming replacement capability. As updates are available to this schedule, the PMO should share and coordinate directly with JITC and JRSS stakeholders to support risk assessments and continuous monitoring activities, as well as DOD Component planning, until the incoming capability is fully adopted.
3. JITC and the DOD Components should collaborate to identify and implement meaningful metrics in JITC's continuous monitoring reports.
4. The JRSS PMO and JITC should implement a method to ensure that any new capabilities and upgrades are evaluated via risk-based analyses to support the continuous monitoring test strategy.
5. The JRSS PMO, DOD Components, and JITC should proceed with the planning of an Adversarial Assessment against JRSS, inclusive of the new SIEM 2.0 capability.
6. DISA should assure adequate test funding to support a successful operational transition from JRSS to the incoming replacement capability.