DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

JRSS Discussion Panel

Joint Regional Security Stack

Chair COL Greg Griffin
JRSS Portfolio Manager
May 2018

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

JRSS Priorities and Way Ahead

- Currently, the Army, the Air Force, the Navy, the Coast Guard, two COCOMs and a number of Joint entities have begun their migrations. JRSS has two tiers of protection– agency tier and base tier. The majority of the Army, Air Force, and COCOMs will have completed both tier one and tier two migrations by the end of fiscal year 2019.

- Key Priorities:
  - Provide world class execution from funding to post-migration
  - Maturity of the operational environment
  - Deliver continuous upgrades of industry leading capabilities
  - Reduce the footprint of the stacks through aggressive virtualization
  - Advocate for sufficient resources and execute them effectively

Joint Regional Security Stack (JRSS)

- Complementary defensive security solutions that:
  - Remove redundant cybersecurity protections
  - Leverage enterprise defensive capabilities with standardized security suites
  - Protect the enclaves after the separation of server and user assets
  - Provide the tool sets necessary to monitor and control security mechanisms
- Addresses immediate needs:
  - Defend the cyber warfighting domain
  - Shrink attack surface
  - Standardize security architecture
  - Streamline Command and Control
  - Synchronize Global Network Operations

Installed JRSS

JRSS Value Proposition = Security + Network Modernization + Cyber SA

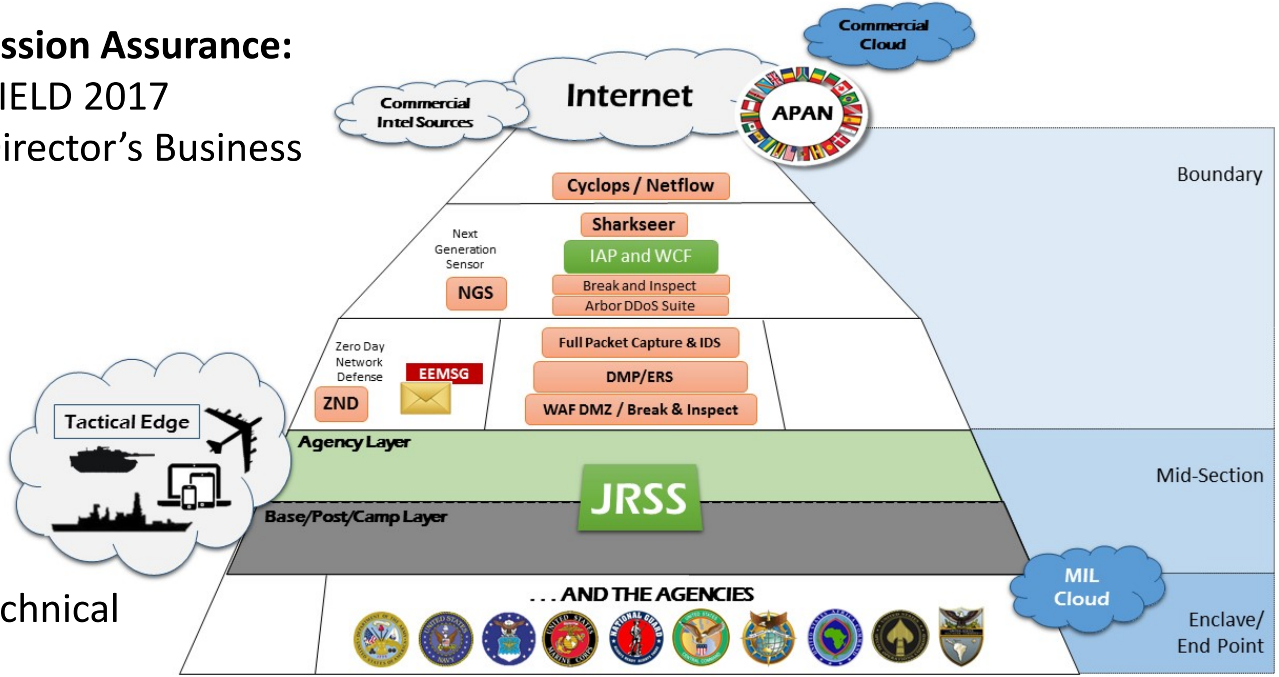
DISA Global Operations Command (DGOC)

- Network Operations Mission:
  - Operate and maintain JRSS stacks
    - Global C2 of JRSS/JMN/JMS
    - OS, patch, and fault management
    - Operate, manage, and maintain all JRSS equipment
    - Support the optimization of the network
    - 24x7, Tier 1 & Tier 2
- CSSP Mission:
  - Joint Management Network defense
  - DISA CSSP customer defense (SLA dependent)
  - 24x7, monitor, detect and defend
- Access Management:
  - Creation/Maintenance of all accounts for each agency
  - Troubleshoot users accounts and permission issues

Operate and Maintain – Fight the Fight

JFHQ-DODIN’s Global Responsibility & A Few Key Efforts

- **Operational Effectiveness - Mission Assurance:**
  - OPERATION GLADIATOR SHIELD 2017
  - Cyber as Commander’s & Director’s Business
- **Priorities & Readiness:**
  - Cyber Tasking Cycle
  - JFHQ-DODIN Operations Center
  - Predictive Intelligence
- **Integrated Expertise:**
  - Cyber Operations, Joint Operations, Intelligence, Technical
- **Partnerships & Collaboration:**
  - Common Awareness to Reduce Global Risks



Synchronize the Fight Across All 42 DOD Components

DISA Defensive Cyber Operations (DCO) CE2

- Mission: DISA DCO team standardizes, synchronizes and supports Defensive Cyber Operations within JRSS

- Priorities:
  - Provide recommendations to JRSS PMO and JFHQ-DODIN on DCO capabilities within JRSS
  - Participate in the policy and governance process to provide operational perspective to the DoD DCO community at large

- Efforts:
  - Developing JRSS DCO TTPs and best practices
  - Working with JRSS stakeholders to identify and resolve operational issues (JRSS DCO WG)
  - Supporting JRSS optimization efforts

Consolidating operational input to drive and influence policy, governance, and Defensive Cyber Operations in the JRSS environment

JRSS Priorities and Way Ahead

- Looking ahead, the vision for JRSS is to ensure that All DOD traffic moves seamlessly along well defended, flexible enterprise networks.
  - The network operators and maintainers have the right information presented in a meaningful way to proactively anticipate conditions that lead to outages and mitigate them before they impact service to the user.
  - JRSS will also present network defenders with critical information in a meaningful way to proactively adjust defenses to protect against the newest threat vectors and be able to detect adversaries already in the network and stopping them from disrupting our communications.

- At end state, JRSS will deliver to the greater DoD community the ability to act uniformly with predictable outcomes through this centralized, standardized, and modernized infrastructure. Service, COCOMs, and Agencies will be able to see more, defend more easily and share information seamlessly both within their organization and externally to their fellow DoD mission partners.

Information Resources

DoD CIO wiki (CAC required):

https://www.milsuite.mil/wiki/JRSS

JRSS Portal (CAC required):

https://disa.deps.mil/ext/cop/mae/cop_mae/JRSS/SitePages/Home.aspx

Contact email:

disa.meade.id.mbx.jrss-jmt-gov-leads@mail.mil

rate us

take the **3-question** survey available on the AFCEA 365 app

visit us

DISA Booth # **443**

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**