DISA

Summer 2018 Look Book

JRSS
Joint Regional Security Stacks

GPIs
Global Private Internets

MNIS
Multinational Information Sharing

DMCC-S
DOD Mobility Classified Capability - Secret

Assured Identity

NBIS
National Background Investigation Services

Joint Regional Security Stacks (JRSS) – Cyber Defense

Overview:

JRSS includes a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding, as well as other network security capabilities.

The physical “stack” in JRSS is comprised of 20 racks of equipment that allow for big data analytics, which enable DOD to intake large sets of data and provide the platforms for processing the data, as well as the mechanisms to help analysts make sense of the data.

As network traffic – including large sets of data – moves through these stacks, network defenders and operators are able to see every packet, or unit of data, being routed through the network.

Army COL Gregory C. Griffin
JRSS Program Manager

JRSS vision for the future:

- All DOD traffic seamlessly moving along well defended, flexible enterprise networks.
- Network operators and maintainers have the right information presented in a meaningful way to act proactively, anticipating conditions that lead to outages and resolving them before they impact service to the user.
- Network defenders have the right information presented 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 stop them from disrupting our communications.

Status

Currently, the Army, the Air Force, a number of joint entities, and several combatant commands (COCOMs) have begun their JRSS migrations. JRSS has two stages: agency level protection and base level protection. The majority of the Army, Air Force, and COCOMs will be complete with stage one and two by the end of fiscal year 2019.

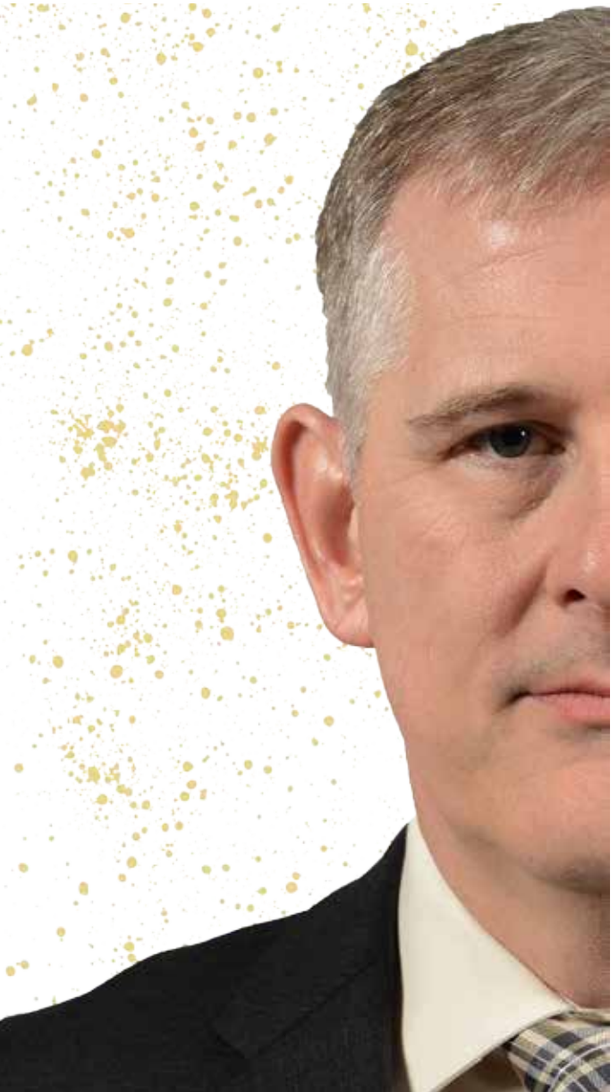
Why is JRSS Important?

JRSS provides tools and the best defended unclassified networks in the world by some of the best network defenders in the world. There is a 100 percent failover within the JRSS with an A-side and a B-side that will appear seamless to the user. If the second failover is compromised, there is a secondary failover to another A-side and B-side. Additionally, customers have a third failover so that makes a six-failover barrier system before traffic would truly stop. This creates a secure environment that is next to impossible to fail.

How will JRSS make things better for our mission partners?

In September 2017, the DISA Joint Migration Team (JMT) began working hand-in-hand with the military services and DOD agencies to ensure government representation throughout the JRSS program life cycle. The main purpose of the JMT is to support the military departments, COCOMs, and DOD agencies migrating to JRSS. This includes supporting the Migration Planning Board (MPB) activities, collaborating with subject matter experts from across DISA, DOD Chief Information Officer (CIO), and JMT, and ensuring that the appropriate level of access is available to the migration teams.

Global Private Internets (GPIs)



Overview:

How does DOD achieve reliable and guaranteed on-demand universal transport capability between any two commercial endpoints worldwide?

GPI endpoints are not only traditional carrier demarcation points that we know as base/post/camp/station, but will include non-traditional locations on college campuses, commercial data centers, co-location facilities, conference centers, business parks, malls, offices, and hotel rooms. This capability is survivable in the event of a large scale internet outage where commercial connections are isolated from the internet and are actively managed/guaranteed.

David Stern
Electronics Engineer
Software Defined Networking Expert

How will your program innovate or deliver innovative solutions?

The program has already achieved some significant milestones. First, it won a Carrier Ethernet 2.0 award at Metro Ethernet Forum (MEF) 2017 for its work in cooperation with the first commercial service provider in developing the Application Programming Interfaces (APIs) to effectively control that carrier's network for the DOD's intent. Second, DISA open sourced the main portions of the code used for this program through the Defense Digital Service on GitHub.com. Third, this was the first time that DOD used a portion of an existing connection to a provider to provision services with that provider directly, and on-demand.

The innovation enables the agency to deliver commercial services that may or may not transit DOD infrastructure, on demand and within minutes.

Why is your program important?

This dual-use technology is being developed to benefit national interests for civilian and defense needs. For humanitarian operations, GPI can serve the world by integrating the best network, compute, storage, and security capabilities that the world has to offer. This technology also provides the ability to integrate disparate systems and capabilities into a managed commercial capability that meets both privacy and security requirements.

How will your program make things better for mission partners?

Agility in provisioning global private internets will be the key to maneuvering within the cyber domain of warfare. Our mission partners require access to the best network, compute, storage, and security that the United States and the world can offer. GPI integrates several of those capabilities and shows great promise in promoting mission partner lethality through cyber maneuver enablement.

Multinational Information Sharing (MNIS)

Overview:

Multinational Information Sharing (MNIS) is a division within the DISA Infrastructure Directorate that consists of a portfolio of initiatives to improve interoperability and information sharing between DOD components and foreign nations or coalition partners.

MNIS provides a number of services that deliver significant value to our customers.

- Rapid deployment and testing of command and control operations between allies and mission partners.
- Seamless integration and leveraging of existing DISA enterprise solutions and services.
- Responsive service management and a common Network Operations (NetOps) view of our systems.
- Dynamic enhancements and modernization to existing capabilities and services.

Heidi Cotter
Chief, MNIS

What is on the horizon for your program?

MNIS is continuing to work with the DOD CIO, joint staff, combatant commanders, and military services to enhance coalition capabilities that support the vision of an integrated Mission Partner Environment (MPE). The objective of MPE consists of delivering a global, enterprise, virtualized full-service platform that will enable enhanced command and control operations with our mission partners.

How will your program innovate or deliver innovative solutions?

One of our key MPE programs is the Virtual Data Center (VDC). DISA has deployed strategically-placed VDC nodes where multiple discrete mission enclaves will be converged on a single platform while maintaining distinct virtual network separation.

This innovative new way of sharing operational and intelligence information between nations enable rapid deployment of mission support services and meet “fight tonight” rapid response required by today’s warfighters.

We are continuing to strategically add new VDC nodes and stand up mission enclaves to meet increased requirements for this type of service.

Another program innovation is to provide an enhanced research, development, testing and evaluation environment for U.S. and coalition partners. We are currently in the process of integrating all the various networks into a singular coalition testing lab environment housed at DISA to support the pre-production tests of technologies for assurance, interoperability trusts, and ease of transition to operations.

DOD Mobility Classified Capability - Secret (DMCC-S) Windows 10 Tablet

Overview:

The DOD Mobility Program Management Office is working on a unique development of the first ever DOD Mobility Classified Capability - Secret (DMCC-S) Windows 10 tablet. The pilot will leverage existing DMCC-S infrastructure and the tablet will conform to the National Security Agency's (NSA) Data At Rest Capability Package.

Neil Mazuranic
Chief, Mobile Capabilities Development

What is on the horizon for your program?

The Windows 10 tablet pilot is scheduled to begin fielding in the summer of 2018. The capability will provide a native email experience, video conferencing, access to the Global Command & Control System – Joint application, limited web browsing on the Secure Internet Protocol Router Network (SIPRNet), and secure voice calls to Defense Red Switch devices.

How will your program innovate or deliver innovative solutions?

The DMCC-S Windows 10 tablet will be the first enterprise capability developed and fielded according to NSA's Data At Rest Capability Package. This tablet will provide a level of flexibility, convenience, and effectiveness not yet seen in the classified arena because the device will provide a native Windows experience while on the go. Additionally, the tablet will be Unclassified/For Official Use Only (U/FOUO) when powered off and not secret.

Why is your program important?

Our pilot will be the first to leverage NSA's Data at Rest Capability Package and will pave the way for others to follow with their own development. The pilot is a proof of concept, designed to show that truly mobile classified solutions are achievable.

How will your program make things better for mission partners?

The Windows tablet pilot will serve as a guideline for mission partners to follow as they develop their own classified Windows solutions.

Assured Identity

Overview:

Assured Identity is the concept of establishing and continuously validating a digital identity, assigning attributes to that identity, and strongly associating it with an individual or trusted device.

DISA is addressing this initiative by prototyping hardware attestation on mobile devices and two separate prototypes of continuous multi-factor authentication (CMFA).

Jeremy Corey
Chief, Cyber Innovations

What is on the horizon for your program?

Assured Identity is actively piloting a continuous authentication technology that measures a user's keyboard and mouse dynamics.

In April 2018, DISA piloted an authentication concept reliant on a wrist worn device in conjunction with a mobile device and a user's computer to validate assumptions regarding user experience and repetitive authentication during normal office work activities.

In October 2018 our largest pilot ever will commence with 75 commercial reference devices to observe users' adoption of a mobile device for authentication in lieu of a common access card (CAC).

How will your program innovate or deliver innovative solutions?

Assured Identity is one of several projects in Cyber Innovations and demonstrates how we exercise our three phase methodology of identifying problems, brainstorming, experimenting, and lastly, operationally transitioning the solution.

Why is your program important?

At the highest levels of the Department and highlighted in the National Defense Strategic objectives, we are building for the warfighter by evolving operational concepts and delivering value at the speed of relevance. Our program emphasizes on failing fast and at low cost. We continuously pivot in order to anticipate implications of new technologies to the warfighter and provide just enough information for calculated financial and security risk-taking.

How will your program make things better for mission partners?

Meeting with our mission partners, understanding their problem sets and use cases, and constantly tapping into non-traditional defense contractors and small start-ups, we quickly assess the viability of technologies while simultaneously refining mission partner requirements.

National Background Investigation Services (NBIS)

Overview:

In the second quarter 2016, Congress charged DISA to lead an effort in collaboration with the Office of Personnel Management (OPM), the Defense Contract Management Agency (DCMA), and other DOD agencies to design, build, test, field, operate, maintain, and secure a suite of National Background Investigation Services.

NBIS is intended to provide a capability for the entire federal government. There are seven critical functional requirements for NBIS:

- Ability to designate position sensitivity.
- Ability to collect and validate investigation data from users.
- Provide a solution for managing investigations.
- Provide fingerprint and biometric processing.
- Improve automated record checking.
- Facilitate adjudication.
- Perform continuous evaluation.

Raju Shah
NBIS Program Manager

What is on the horizon for your program?

National Background Investigation Services (NBIS) will contain personal information for more than 22 million people, with the DOD representing roughly 75 percent of applicants. Its purpose is to facilitate and secure the process for determining the suitability of individuals to access our nation's critical information.

NBIS will automate a number of previously manual processes to enable investigators to spend less time gathering and synthesizing information from various sources and more time assessing that information. By leveraging dynamic forms, re-applicants will find relevant fields pre-populated with data from previous applications.

NBIS streamlines the process of conducting federal background investigations and secures investigation data within the DISA Defense in Depth Ecosystem, assuring employees, citizens, and contractors of the security of their personal information.

Continuous evaluation will transform the process from relying heavily on periodic reinvestigations to providing ongoing checks that will alert investigators to any possible changes in circumstances that prompt a new investigation.

What is on the horizon for your program?

In addition to continuing to automate the currently manual information collection portions of security investigations, NBIS is funding research and development in the creation of faster and more accurate algorithms for analyzing the investigative data. This will further improve the overall investigative and adjudicative quality of the system while also reducing the lag time between requesting and receiving (or being denied) a clearance.

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil