

FALL LOOK BOOK

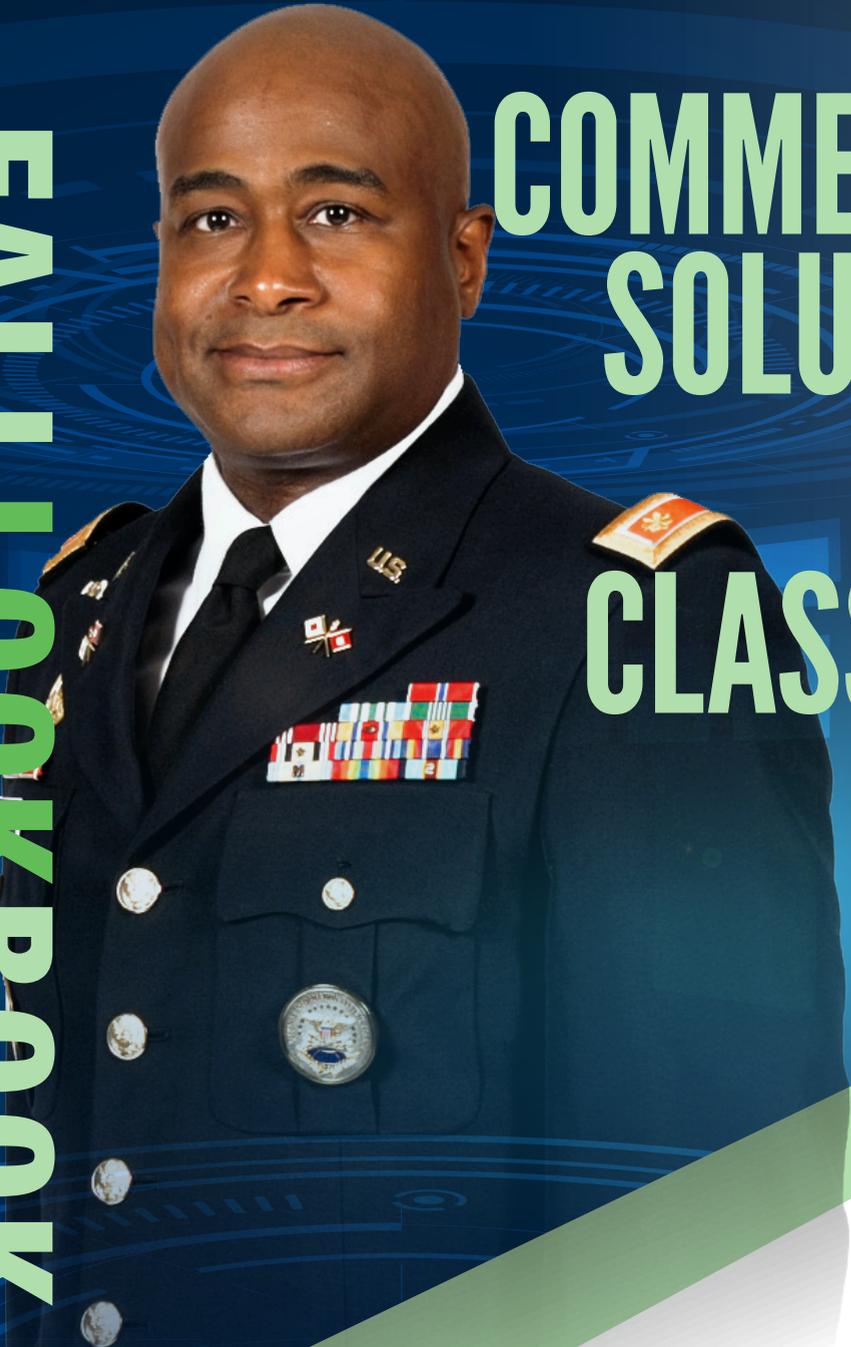


- Commercial Solutions for Classified (CSfC)
- Joint Cyber Implementation Program (JCIP)
- Domain Name System (DNS)
- Defense Red Switch Network (DRSN)
- The Global Content Delivery Service (GCDS)
- Unified Video Dissemination System (UVDS)
- All Partners Access Network (APAN)

2018 A NETWORK VIEW



COMMERCIAL SOLUTIONS FOR CLASSIFIED CSfC



Major Francisco Ortiz, USA
Program Manager,
Commercial Solutions for
Classified

Originally developed by the National Security Agency (NSA), Commercial Solutions for Classified (CSfC) is a strategy for leveraging industry innovation to deliver information assurance (IA) solutions efficiently and securely. CSfC is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of applications. CSfC allows the deployment of commercial-off-the-shelf (COTS) solutions, with encrypted data protection, at a fraction of the time and cost of more sensitive Type-1 encryption products.

Within DISA, the CSfC Program Management Office (PMO) is working with DISA field offices, combatant commands, joint staff, and military services to enhance capabilities that support the vision of an enterprise CSfC solution. The objective of the enterprise CSfC consists of delivering a secure, global, enterprise, service-platform that will enable secure communications using a diverse set of commercial products.

The CSfC PMO is working on an initial pilot that will leverage and converge existing DOD Mobility Classified Capability – Secret (DMCC-S) and Enterprise Classified Travel Kit (DECTK) infrastructure to deliver a cost effective and mission centric CSfC solution.

CSfC provides a capability to access secure communications from multiple devices, anywhere, and at any time, for greater mission effectiveness. CSfC will feature a robust enterprise public key infrastructure (PKI) management system, with the ability to issue and revoke PKI certificates to/from our customer base. This feature will also allow customers to connect their existing CSfC enclaves to our enterprise CSfC enclave and access their secure systems and networks.

CSfC harnesses the power of commercial industry, providing a secure alternative for government-off-the-shelf (GOTS) IA solutions. CSfC allows customers to keep pace with technological progress, while reducing the time it takes to build, evaluate, and deploy IA solutions. Potential cost savings may be realized through marketplace competition and rapidly deployable, scalable commercial products.

Our mission partners increasingly require immediate use of the market's most modern commercial hardware and software technologies, in order to achieve mission objectives. CSfC leverages emerging technologies to deliver more timely and cost effective IA solutions for rapidly evolving customer requirements.

JOINT
CYBER
IMPLEMENTATION
PROGRAM
JCIP

Major Gilbert Kofie, USA
Chief, Joint Cyber
Implementation Program

The Joint Cyber Implementation Program (JCIP) employs a team of highly skilled Air National Guard IT professionals to engineer, install, and enable DOD information-sharing capabilities and information infrastructure in support of joint warfighters, national-level leaders and other mission and coalition partners across the full spectrum of military operations.

Our near and long-term objectives are to continue to operate with a continuous focus on process improvement and cost savings. Furthermore, we will continue to provide consistent, reliable, and professional site implementation services to our customers and mission partners.

JCIP is unique in its make-up. It is comprised of Air National Guard members based out of a network of partner units located throughout the continental United States. JCIP's engineers, surveyors, and installers are pulled exclusively from the Air Force's Engineering and Installation (EI) Squadrons. In addition to providing a ready-made pool of talented IT technicians, the EI community supports DISA cost savings by providing their own workspaces, administrative support, and regular training at the member's home station.

JCIP minimizes implementation costs by using military support in lieu of contracts. Using military support introduces efficiencies in travel costs and response times by having skilled technicians prepositioned across the country. The use of National Guard members on active duty tours provides valuable flexibility in the field to react to changing site conditions, scope of work, and project durations without the necessity of contract or task order modifications.

The Joint Cyber Implementation Program is not a replacement for using contractor support. Rather, we provide project stakeholders with a flexible option to augment traditional contract vehicles for project execution. JCIP is able to react quickly, often being onsite within 24 hours, to a wide range of implementation activities worldwide.



DOMAIN NAME SYSTEM DNS

Jill Place
Chief, DNS Network
Information Center

The Department of Defense (DOD) Network Information Center (NIC) has several mission areas that support the warfighter. The most utilized is a translation technology called DNS or Domain Name System. DNS is a protocol standard developed by the Internet Engineering Task Force. It allows users to type a website name into an internet browser and link to the network address of computers that contain the information they are requesting. DNS is a technology that allows the warfighter to access content located anywhere in the global Internet.

We have two sequences of technical refresh projects that will upgrade the hardware supporting DNS functions at both the internet and the DOD levels of the protocol. The hardware upgrade will allow us to improve our ability to collect and analyze performance statistics as well as respond to more complex cyber operations requirements.

The technical refresh to this upgraded environment will allow us to expand our performance statistic capabilities and assure DISA's ability to continue to operate at the performance levels required for a global internet root server provider. The operating system will also allow the NIC and the DNS Hardening Program additional flexibility in implementing new defensive cyber operation measures across the DNS architecture supporting the Department of Defense Information Network (DODIN).

Without a translation technology like DNS, users of the internet and the DODIN would be required to memorize or maintain manual lists of the complicated internet protocol (IP) network addresses of every content site or application they need. Our current model of user-transparent network changes would be ineffective without the flexibility of DNS. IP network function would be slower and more difficult for our warfighters without DNS.

DNS capabilities are an integral function of any network infrastructure. DISA will operate the DNS at the highest performance levels across our networks and continually seek to improve defensive cyber operations related to DNS to alleviate this burden on our mission partners so they can concentrate on mission objectives. In addition, by maintaining a presence within the international technical community as a root server operator, DISA assures DOD has a voice in shaping the future of global communications.

DEFENSE RED SWITCH NETWORK DRSN

Stanley Wooten
Branch Chief,
Communication
Gateways Branch

The Defense Red Switch Network (DRSN) provides the DOD with high-quality secure voice telephone and conferencing services for end-to-end use by DOD authorized users. The DRSN includes a range of assured services to command and control (C2) users and their missions in an environment of a robust and feature-rich set of capabilities. This service provides major facilities to include the National Military Command Center and Combatant Command headquarters with interconnections through a cryptographically secured network. The DRSN uses the Digital Small Switch (DSS-2A) red switches for multi-level secure calls and conferencing and uses Promina equipment for Time Division Multiplexed (TDM) transport. The Promina equipment is at end-of-life and end-of-service and requires a replacement transport. The DSS-2A switches will provide an Internet Protocol (IP) interface connection to IP routers, which will interface with IP encryption for secure IP transport.

On the horizon:

- Replace the end-of-life and end-of-service Red Promina Time Division Multiplexed transport network with an IP at 45 different sites.
- Migrate DRSN inter-switch trunks from circuits to IP routing to phase out TDM transport among DRSN voice switches.
- Transition multilevel secure voice users to enterprise classified Voice Over Internet Protocol (VoIP) service.
- Provide two network and security operations centers for network management and security management.
- Upgrade the Digital Small Switch (DSS-2A) switch with IP cards and new software for IP integration.

This transition of the DRSN from the Time Division Multiplexed transport to Internet Protocol will increase capacity (from T-1 to 1Gbps or 100Mbps circuits) and security (multi-layer proactive security) and improve scalability, with the ability to support higher call volume, and greater functionality. An IP based infrastructure will provide cost efficiencies by eliminating the need to support TDM technologies and provide a more resilient and secure network.

The DRSN program has delivered innovative solutions by using a full life-cycle methodology from initiation of the project to closeout. The DRSN IP solution undergoes rigorous test and evaluation from the vendors, lab, and Joint Interoperability Test Command (JITC) and site testing from the early phases of the project life cycle throughout deployment, implementation and sustainment. The project manages and mitigates risk along the life span of the project to minimize user impact. The transition to IP will have a dual period where TDM and IP will be in parallel. Once IP is feasible the system will migrate to IP.

This program is very important for DOD Global Secure Voice System (GSVS) during peacetime, crisis, or even conventional war. DRSN provides the core service of GSVS.

The Global Content Delivery Service (GCDS) is a type-accredited DISA enterprise managed service, which provides performance, security, and infrastructure reduction to its Department of Defense (DOD) mission partners. For over a decade, it has helped the Department of Defense Information Network (DODIN) scale to meet its application and infrastructure challenges by operating a powerful multi-tenant and fully managed web fabric.

The next phase of the project is scoped to expand upon the existing GCDS fabric with a broader platform and additional infrastructure. This will allow for a distributed approach to traffic shaping and cache hierarchy for commercial content consumed on Non-classified Internet Protocol (IP) Router Network (NIPRNet). The approved enterprise solution will help alleviate pressure experienced on the internet access point (IAP) infrastructure by reducing bandwidth via multiple strategies that target specific applications including high-definition video streaming and social media.

GCDS is highly available and fault tolerant, using multiple layers of real time network measurement and capacity utilization to efficiently spread load across the system. A number of optimizations are used to help reduce bandwidth at the IAPs, such as caching, server-side throttling and client optimizations.

The existing and operational GCDS service was configured to help ease the pressure experienced at the IAPs by focusing on a percentage of the commercial traffic bandwidth handled at the gateways. By utilizing currently fielded capacity, the GCDS service is operationally ready to support the IAP mission on day 1.

Due to the explosive growth in demand for high-bandwidth content such as software updates, high-definition video, and social media, the bandwidth demand on DISA's IAP infrastructure increases rapidly and necessitates expensive upgrades for cybersecurity inspection devices and transport infrastructure to keep pace. Historically, planning for bandwidth expansion and/or network optimization at the IAPs is a known and cyclical challenge as the incremental increase in bandwidth consumption exceeds the infrastructure's thresholds. These results in capacity constraints while serving traffic and service degradation with congestion across the enterprise. Exponential rate of traffic growth at the IAPs presents a growth challenge for the enterprise.

Previously, GCDS's proof-of-concept (POC) successfully applied bandwidth reduction capabilities to specific commercial internet applications on DISANET at Fort Meade without any negative impact to end users. Multiple bandwidth reduction techniques were applied to the applications and we demonstrated a bandwidth reduction of 42 percent and 99 percent for applications, such as YouTube and Certificate Revocation Lists (CRLs) respectively.

Due to the success of the proof-of-concept, DISA approved GCDS as an enterprise solution for reducing bandwidth at the IAPs across the DODIN and beyond DISANET. Capacity buildout is underway in CONUS and OCONUS to deliver the heavy hitter internet properties; meanwhile, GCDS is already delivering 2TB of commercial CRL traffic across the DODIN and reducing its bandwidth by 99.97 percent at the IAPs.

THE GLOBAL CONTENT DELIVERY SERVICE GCDS



Tobi Felder
Chief, Global Content
Delivery Service Branch

The Unified Video Dissemination System (UVDS) provides a temporary hosting of manned and unmanned sensor platform, full motion video and data product feeds. We currently host US-NOFORN and Five Eyes (FVEY) products, and host a limited number of coalition feeds on Secure Internet Protocol Router Network (SIPRNet) and Wide Area Network (J-WAN) enclaves.

There are two things on the horizon for Unified Video Dissemination System. We are moving through the Joint Capabilities Integration and Development System (JCIDS) process, and the Airborne Intelligence, Surveillance and Reconnaissance Initial Capability Document is proceeding through Pentagon staffing. The initial capability document itself is broken into four blocks, with the first block using UVDS as its basis. We are taking blocks 2, 3 and 4 through the staffing process in the same deliberate manner over the next three years.

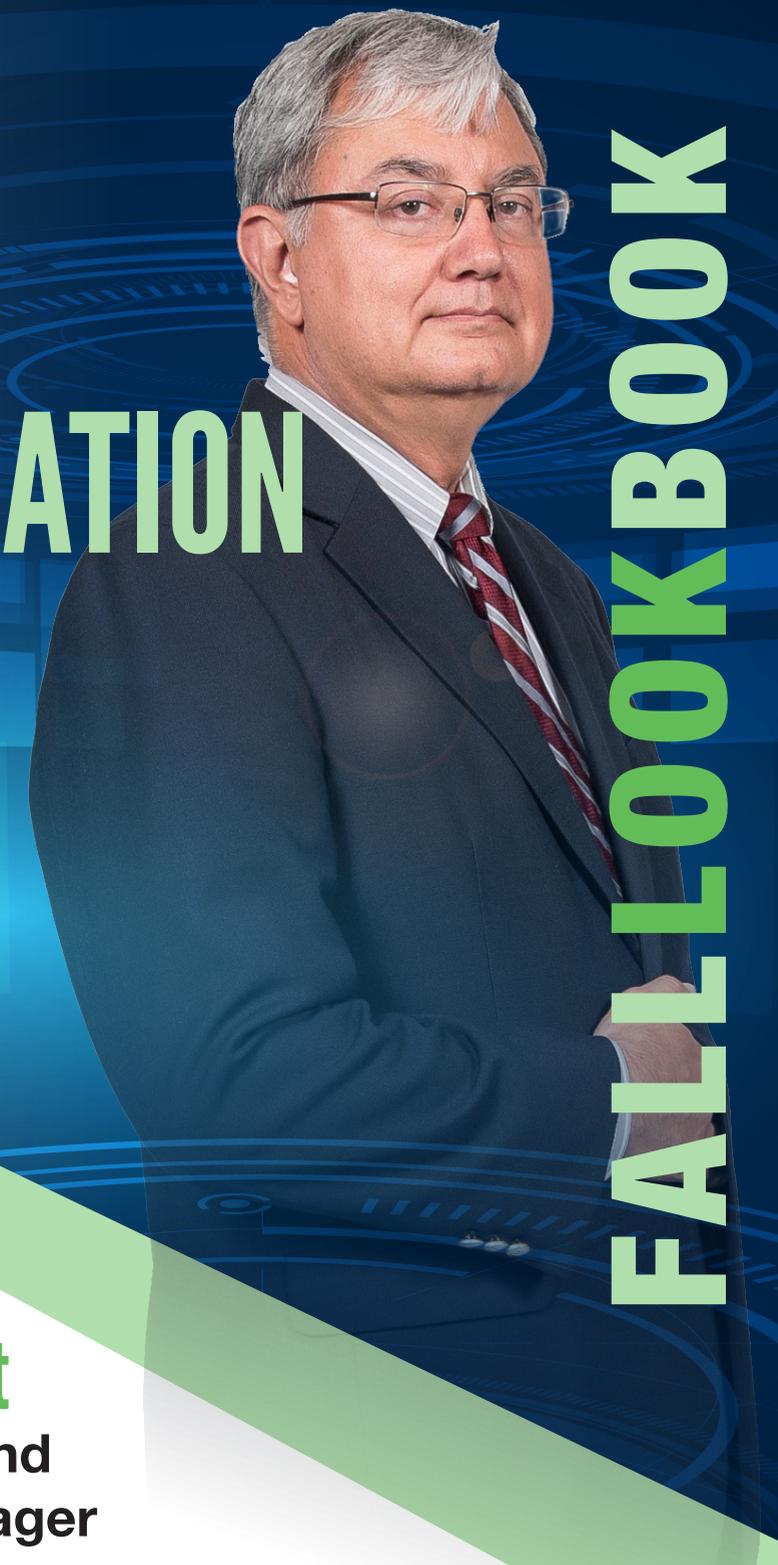
We are moving from the nomenclature of UVDS to USDS (Unified Sensor Dissemination System) to show the continued modernization of the program and the support for ground, afloat and underwater sensor platforms.

This program has innovated solutions by working very closely with the J2, J3, and J6 proponents (U.S. Southern Command, U.S. African Command, U.S. Central Command with U.S. Europe Command and U.S. Pacific Command coming on board) and fielded transrating and transcoding devices to match algorithmic upgrades. Our team is working on the support for the move from standard to high definition and ultra-high definition (4K) video. We have teamed with the DOD Mobility Program on supporting the classified video environment through their classified devices.

This system provides the commanders an accurate and relevant environment to operate and execute orders. Commanders can view the battlefield real-time and make critical adjustments to ensure mission success and save lives.

We have already seen the turn from an environment of 100 percent US-NOFORN data, to operating in an 80 percent FVEY environment. Our mission partner's support is essential, and we are meeting their needs.

UNIFIED VIDEO DISSEMINATION SYSTEM UVDS



Robert (Bob) Willett
SATCOM Gateway and
UVDS Portfolio Manager

All Partners Access Network (APAN) is a web-based, unclassified non-dot-mil internet community accessible to the DOD and its mission partners around the globe without the constraints of traditionally closed DOD networks. APAN provides an unclassified information sharing and collaboration platform for sharing information among various government, non-government, state, federal agencies, international organizations, and multinational partners, supporting humanitarian crisis response efforts, multinational and joint exercise planning, working conference groups, and partnership building events.

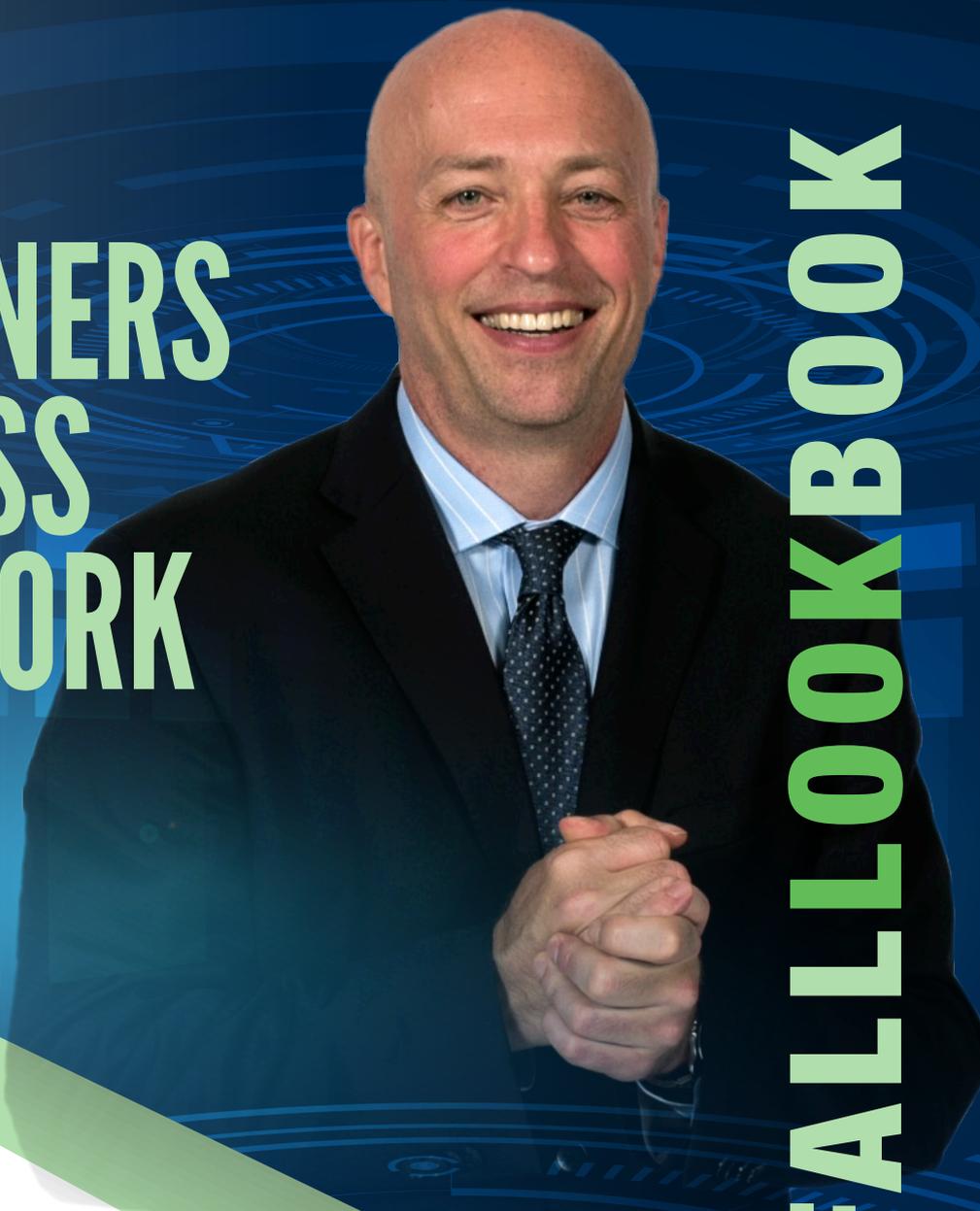
The APAN program is the premier U.S Department of Defense unclassified information sharing and collaboration service. There are 184,246 total registered users across the globe. APAN is utilized within federal and state agencies, the services and National Guard, and all nine combatant commands (CCMDs). If there is a humanitarian or disaster response anywhere on the globe, it's likely that APAN will be used to generate and manage the response efforts. For example, APAN was used during flood responses in both Florida and Texas in 2017.

The APAN program was originally conceived and implemented to allow mission partners and hosted communities to collaborate, communicate, and synchronize efforts across the globe. APAN is a robust capability that host various services to include blogs, wikis, virtual conferencing, geospatial/mapping, language translation, chat, email, and document management.

- Chat - provides instant messages to collaborate with team members or APAN communities of interest.
- Translation - facilitates communication with foreign partners in real-time in 18 different languages.
- Maps/ Geographic Information Systems (GIS) - enables the creation of interactive maps and the sharing of geographically tagged information to enhance situational awareness.
- Adobe Connect – provides connectivity with anyone anywhere to host professional meetings, trainings and seminars.
- Metrics- enables community of interest owners to review usage data specific to each group or site using APAN.

An initiative has begun to transition the APAN capabilities currently hosted at a DISA data center a commercial provider, which includes true failover and fallback capability. The move to the cloud will cost about \$1.8 million. Multinational Information Sharing (MNIS) has fully funded this effort to develop and implement this capability this year. In addition to resolving the resiliency issue, this modernization effort will position the program to remain the premiere DOD tool for information sharing, collaboration, and synchronization as well as humanitarian and disaster response across the globe. The APAN system transitioned to the Air Force Oct. 1, 2018.

ALL PARTNERS ACCESS NETWORK APAN



Dickey Rounsaville
Deputy MNIS Portfolio Manager



