STRATEGIC EFFORT

OPERATE AND DEFEND THE DODIN

ADOPT–BUY–CREATE

ENABLE PEOPLE

REFORM THE AGENCY

INNOVATION

CUSTOMER SERVICE
OPERATE & DEFEND
The Defense Information Systems Agency (DISA) has adopted a unified computing ecosystem that maximizes the use of resources and capabilities across DISA’s entire computing enterprise, enables DISA to standardize processes and services, and allows the agency to offer our mission partners increased capabilities and savings in the future.

The ecosystem addresses mission partners’ need for more efficient solutions at lower rates. The ecosystem aligns like functions across a single computing enterprise and establishes a unified computing structure that operates under a single command. The ecosystem also expands the availability of technology and resources across the entire computing enterprise.

As the agency continues to evolve the ecosystem structure, cost savings will be passed on to mission partners in the form of rate reductions.

Communications
Provides the strategic vision for the Defense Enterprise Computing Centers (DECCs) and sustains the DECC communications infrastructure.

Cyber
Responsible for implementing the cyber policies impacting computing and for addressing the information security requirements necessary for operating an optimized computing environment.

Data Center
Responsible for capacity management - enabling the Department of Defense (DOD) components to monitor, scale, replace, and enhance their capacity quickly and dynamically, while staying abreast of the newest technologies and offering the most efficient and cost effective solutions.

Implementation & Sustainment
The gateway to DISA’s computing ecosystem - manages the implementation and sustainment of all mission partner workloads to full operational capability using a standard infrastructure that provides information superiority to mission partners.

Infrastructure
Maintains and sustains storage, virtualization, change and configuration capabilities in an operationally effective and efficient manner in support of DISA’s data centers and mission partners.

Mainframe
Provisions, secures, operates, and maintains all mainframe hardware, storage environments, operating systems, databases, and independent software vendor products.

Server
Delivers a reliable, standardized computing environment through the implementation and sustainment of the operating systems and associated enterprise management tools within DISA’s inventory.

Special Services
Offers customized enterprise computing capability and support to include integration, sustainment, tiered-level support, and security remediation to DOD mission partners.
ACTIVE – ACTIVE OPERATIONS

DISA is moving to Active-Active operations. DISA Global Operations Command (DISA Global) will function as one Command, operating from two locations: Scott AFB, Illinois and Hill AFB, Utah.

The two locations will jointly operate and secure the Defense Information Systems Network (DISN), ensuring real-time redundancy of the network globally.

• DISA Global currently works within a continuity of operations model should a contingency arise. By moving to Active-Active operations, DISA Global can fully operate the DISN 24/7 from either location if required.

• Active-Active increases DISA’s capacity for providing secure operational capabilities.

• Active-Active enables advanced defensive cyber operations (DCO) and Joint Regional Security Stack (JRSS) capabilities.

• Active-Active will incorporate the Enterprise Virtual Watch Desk (EVWD) concept. Through the use of a suite of real-time collaboration capabilities, EVWD will allow seamless interaction across all operational elements and provide a common operational picture across the DOD Information Network (DODIN).

• Sustained operations at both locations provides mission partners greater assurance that DISA’s service to the warfighter will be “always on.”

• Replication of DISA Global skills, tools, and privileges at a second location allows DISA to make the DISN and DISA services more agile and responsive.

DISA COMMAND CENTER

In order to optimize DOD’s world-class enterprise infrastructure, DISA is focused on providing enterprise services, unified capabilities, and mobility options to support DOD operations anywhere, anytime.

Through enterprise security architectures, smart computing options, and other leading-edge information technology (IT) opportunities, DISA remains committed to its role of the IT provider to meet our defense needs.

In addition, DISA operates the DISA Command Center (DCC), which maintains situational awareness of all network operations and the DISA-provided infrastructure, computing, and enterprise services. This center ensures continued quality customer service to all of DISA’s mission partners.

Support includes:

• Computer network defense information assurance (IA).
• Policy management.
• Incident management.
• Compliance and vulnerability management.
• Forensics management.
• Disaster recovery.
• Continuity of operations (COOP) services.
• Situational awareness.
• Real-time incident response.
JOINT SERVICE PROVIDER (JSP)

JSP provides the full range of information technology equipment, services, solutions, and customer support to the Office of the Secretary of Defense, the Office of the Deputy Chief Management Officer, and Washington Headquarters Services (WHS) to meet mission and business requirements.

JSP’s holistic approach to IT management leverages top talent across the DOD to deliver dependable IT services, enhance network security, and reduce overall IT costs. JSP’s support ultimately ensures that efforts and resources are appropriately allocated toward the Department’s mission success.

GLOBAL SERVICE DESK

The Global Service Desk (GSD) provides warfighters, military components, mission partners, and other federal agencies with a single point of entry for service desk support.

The Service Support Environment (SSE) is a centrally-managed virtual platform that enables a unified process framework with a single ticketing system, a single service request management system, a single call management system, a single quality assurance plan, and a more robust knowledge-centered support structure.

For Help Contact:

1-844-DISA-HLP (1-844-347-2457) or DSN 850-0032.
The Defense Information Systems Agency’s Joint Regional Security Stacks (JRSS) initiative is driving and delivering solutions to network defenders and operators across the department.

With JRSS, the department has, for the very first time, reached a broad agreement that securing the DOD enterprise must be a joint capability. In place of multiple networks at bases, posts, camps, and stations, the JRSS provides the joint capability to protect data and networks in a regional approach.

Having a complete regional picture enables operators and defenders to better understand what’s happening on the network, and enables the various services and agencies to work together and share their analysis of threats and vulnerabilities on a common platform with their peer organizations.

A joint regional security stack is a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding (VRF), and provides a host of network security capabilities. By deploying JRSS, security of the network is centralized into regional architectures instead of locally distributed architectures at each military base, post, camp, or station.

Each physical stack is comprised of racks of equipment which enable big data analytics, allowing DOD components to intake large sets of data to the cloud and provide the platforms for processing data, as well as the mechanism to help analysts make sense of the data.

In addition, DISA is the authorizing official for multiprotocol label switching (MPLS)/JRSS equipment. MPLS is part of a modernization effort to upgrade the bandwidth capacity of the Defense Information Systems Network (DISN). It is also the industry-standard, JRSS-enabling technology that speeds and manages network traffic flow. (More information on reverse).

JRSS allows information traversing DOD networks to be continuously monitored to ensure response time as well as throughput and performance standards. JRSS includes failover, diversity, and elimination of critical failure points as a means to assure timely delivery of critical information.
DEFENSE SPECTRUM ORGANIZATION

DISA’s Defense Spectrum Organization (DSO) supports information dominance by enabling effective spectrum-dependent system acquisition, and spectrum planning and operations. DSO provides commanders direct operational support, including electromagnetic battleground planning, deconfliction, and joint spectrum interference resolution. DSO develops and implements net-centric enterprise spectrum management capabilities to enhance efficiency and effectiveness, and pursues emerging spectrum technologies that may either benefit or impact DOD’s ability to access the electromagnetic spectrum. DSO advocates for current and future military spectrum requirements in national and international forums to protect DOD global operations.

Global Electromagnetic Spectrum Information System (GEMSIS)

GEMSIS is the DSO’s Joint program of record that is transforming spectrum operations from a pre-planned and static frequency assignment into a dynamic, responsive, and agile capability. GEMSIS provides spectrum management capabilities to further enhance the ease of use, efficiency, and effectiveness of spectrum management.

Coalition Joint Spectrum Management Planning Tool (CJSMP)

CJSMP collects unit, platform, and equipment characteristics data for a specific mission or exercise that can be used for analysis and simulation to more effectively manage the electromagnetic environment (EME). It provides spectrum managers with an enhanced capability to identify and mitigate potential electromagnetic interference in an area of interest (AOI).

Joint Spectrum Data Repository (JSDR)

JSDR is a comprehensive repository of spectrum management data supporting sources/web services compliant with the Military Communications Electronics Board (MCEB) Standard Spectrum Resource Format (SSRF) data standard. It provides access to: frequency assignments, spectrum certifications, interference reports, detailed engineering characteristics, and platform employment information. JSDR contains DOD, national, and international spectrum-related information up to the secret level. The JSDR service interface permits machine-to-machine data exchange with other programs requiring access to spectrum data.

Spectrum XXI (SXXI)

SXXI is a joint spectrum management tool for DOD management of radio frequencies. It provides frequency managers with a single information system that addresses spectrum management automation requirements.
Host Nation Spectrum Worldwide Database Online (HNSWDO)

HNSWDO is a web application providing worldwide visibility of host nation radio frequency spectrum dependent equipment’s supportability. It automates distribution of host nation coordination requests and combatant command submission of host nation supportability comments.

End-to-End Supportability System (E2ESS)

E2ESS provides a data collection tool and database for spectrum supportability business processes. Provides worldwide visibility of host nation spectrum dependent equipment’s supportability. E2ESS will integrate and evolve both Stepstone and Host Nation Spectrum Worldwide Database Online (HNSWDO) capabilities to meet GEMSIS E2E supportability requirements.

Stepstone

Stepstone is an online resource for data capture of parametric information for spectrum-dependent equipment supporting the spectrum certification and spectrum supportability processes. It provides a mechanism for the services and industry to complete an “Application for Equipment Frequency Allocation” (DD Form 1494), compliance checks to assure data quality, collaboration and workflow capabilities, and certification process metrics. Stepstone supports the DOD’s equipment spectrum certification process.

Joint Spectrum Center Ordnance E3 Risk Assessment Database (JOERAD)

The Joint Spectrum Center (JSC) Ordnance Electromagnetic Environment Effects (E3) Risk Assessment Database (JOERAD) is a software tool that provides the necessary information to manage the conflict between introduced ordnance and radio frequency (RF) emitters used in joint operations. JOERAD will enable hazards of electromagnetic radiation to ordnance (HERO) safe joint operations by deconflicting potential interactions between ordnance systems and RF emitters.
ADOPT.
BUY.
CREATE.
CLOUD

MILCLOUD 2.0

milCloud® 2.0 connects commercial cloud service offerings to Department of Defense (DOD) networks in a private deployment model to provide DISA mission partners the latest cloud technology at competitive prices without compromising security or performance.

milCloud® 2.0 enables government organizations to consolidate infrastructure while improving continuity of operations while focusing on improved service, enhanced security, and unmatched value.

milCloud 2.0 is a commercial cloud solution, built, operated, and maintained by commercial cloud service providers on DOD property, used exclusively for DOD data and users. By leveraging commercial cloud services, DISA can offer cutting-edge commercial services at a lower cost.

milCloud 2.0 provides an immediate on-premises solution that enables components to reduce hosting costs relative to legacy data storage for applications that are ready for migration to the cloud.

SECURE CLOUD COMPUTING ARCHITECTURE

DISA’s Secure Cloud Computing Architecture (SCCA) is a set of services that provides the same level of security the agency’s mission partners typically receive when hosted in one of the DISA’s physical data centers.

DISA recognized early on the absence of shared security services would be an inhibitor to cloud adoption, so the agency built the Secure Cloud Computing Architecture with a focus on providing those key security services that would allow mission partners to meet their authority to operate (ATO) requirements when moving into the cloud.

SCCA has four components: Cloud Access Points (CAP), a Virtual Data Center Security Stack (VDSS), Virtual Data Center Managed Services (VDMS), and a Trusted Cloud Credential Manager (TCCM).
**CAP**

The CAP is what connects the DISN or the Non-Secure Internet Protocol Router Network (NIPRNet) to the cloud environment. The CAP has two major functions: to provide mission partners with dedicated connectivity to approved Level 4 and 5 commercial cloud providers, and to protect the DISN from any attack that originates from the cloud environment. The CAP is included in the DISN rate, which means there is no direct charge to end users.

**VDSS**

VDSS serves as the virtual security enclave protecting applications and data hosted in commercial environments. It includes two core services: Web Application Firewall (WAF) and Next Generation Firewall. Together, VDSS’s WAF and Next Generation Firewall detect and prevent threats facing web applications and workloads. VDSS is an optional service.

**VDMS**

Management, security, and privileged user access are all handled within VDMS. Five services fall within VDMS, including the Host-Based Security System and Assured Compliance Assessment Solution. They enable mission partners to configure and deliver security policies, push upgrades, and manage roles and security policies. VDMS is where mission partner management workflow path is hosted and is an optional service.

**TCCM**

Offered as a part of VDMS, TCCM can be likened to a virtual system administrator. TCCM includes the processes and procedures to control and monitor privileged user access for cloud environments. DISA provides the checks and balances for mission partners to grant access only to appropriate groups or individuals.
DEFENSE ENTERPRISE OFFICE SOLUTIONS (DEOS)

The Defense Enterprise Office Solutions (DEOS) acquisition of a commercial software as a service solution for unified capabilities is intended to aid the Department of Defense (DOD) in replacing disparate legacy enterprise information technology services for office productivity, messaging, content management, and collaboration.

Using DEOS - a $7.8 billion single award, five-year indefinite-delivery, indefinite-quantity contract vehicle with a five year base period and one five-year option - the DOD can replace systems such as Defense Enterprise Email, the DOD Enterprise Portal Service, Defense Collaboration Services, and many other similar organizationally-provided capabilities.

DEOS will better align resources, processes, and services; enable interoperability between the services and agencies; and leverage the buying power of the DOD for efficiencies of scale.

GLOBAL VIDEO SERVICES

DISA’s modernized internet protocol (IP)-based video teleconferencing (VTC) service, Global Video Services (GVS) provides a full suite of on-demand, high-quality, assured video conference capabilities for users to interact visually within the Non-Secure IP Router Network (NIPRNet) and the Secret IP Router Network (SIPRNet). GVS offers a desktop video solution, allowing face-to-face meetings from the desktop.

Note

A GVS Desktop Client is required to actively control and monitor users in a VTC session.

ENTERPRISE VOICE OVER INTERNET PROTOCOL (EVOIP)

The Enterprise Voice over Internet Protocol (EVoIP) service provides centrally-managed session controllers with a full complement of voice services for use by DOD components. DISA delivers the service offering from the cloud and DOD components can connect to the service using designated hard phones and soft clients validated for placement on the DOD Approved Products List (APL).

This state-of-the-art service, accessible over the Non-Secure Internet Protocol Router Network (NIPRNet) infrastructure, will enable DISA mission partners to decommission their legacy Time-Division Multiplexing (TDM)-based voice switch infrastructure and eliminate other costs associated with managing their local voice infrastructure.
DEFENSE COLLABORATION SERVICES

Defense Collaboration Services (DCS) provides secure web conferencing and instant messaging services on the Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Routing Network (SIPRNet), and is accessible via the Internet.

This open source real time collaboration service is available to more than four million DOD personnel and mission partners and routinely serves 48-thousand web conference users weekly and 16-thousand concurrent chat users daily. DCS resides on milCloud, a datacenter virtualized hosting environment, and supports Common Access Card (CAC) and select hard token holders and guest users (DOD mission partners).

DEFENSE ENTERPRISE EMAIL

The Department of Defense (DOD) Enterprise Email (DEE) service provides secure cloud-based email to the DOD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries. As an enterprise service, DEE reduces the cost of operations and maintenance by consolidating hardware into DISA’s secure, global data center locations. This common platform for DOD ensures mission partners can easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse.

Note

DEE is built on a configurable, multi-tenant environment with the inherent capabilities of Microsoft Exchange 2010.
The Global Command and Control System-Joint Enterprise (GCCS-JE) will be a modernized information technology solution that will replace GCCS-J.

GCCS-JE will provide situational awareness from strategic to operational levels on a globally accessible enterprise cloud-based service that provides a live, fused common operational picture shared in real-time from tactical commanders to the strategic level, and provides intelligence support to operators.

**Capabilities:**

- Cloud based, mobile, enterprise delivery of the common operational picture.
- Web browser and platform agnostic.
- Easier to use with quicker deployment of functionality.
- Lower lifecycle costs to maintain across DOD.
- Cybersecurity is built-in.
- Provides load balancing and new ways to visualize data.
- Enables rapid presentation and aggregation of relevant data to speed decision making.
- Identity and access management data tagged with attributes; access based roles.
Joint Planning & Execution Services (JPES) Portfolio

JPES is a portfolio of capabilities that supports the policies, processes, procedures, and reporting structures needed to plan, execute, mobilize, deploy, employ, sustain, redeploy, and demobilize activities associated with joint operations in order to change the overarching process and transform the way DISA joint operations are planned and executed.

Global Combat Support System – Joint (GCSS-J)

GCSS-J is DOD’s joint logistics system of record, providing access to comprehensive logistics information from authoritative data sources. This access provides the warfighter with a single, end-to-end capability to manage and monitor units, personnel, and equipment through all stages of the mobilization process.

Global Command and Control System – Joint (GCCS-J)

GCCS-J is DOD’s premier joint command and control system of record, providing the joint warfighter with an integrated picture of the battle space supporting all stages of military operations.
The DOD antivirus program supports the operation and defense of the DOD Information Network (DODIN) by providing virus protection to DODIN assets. Currently, the solution licensed by DISA for DOD use is Intel/McAfee AV/AS. This solution can be standardized and deployed both enterprise-wide and on isolated network enclaves (e.g., a tactical environment) to protect laptops, desktops, servers, and e-mail gateways.

**ASSURED COMPLIANCE ASSESSMENT SOLUTION (ACAS)**

The Assured Compliance Assessment Solution (ACAS) is an integrated software solution that provides automated network vulnerability scanning, configuration assessment, and network discovery.

ACAS consists of a suite of products to include the Security Center, Nessus Scanner, and the Nessus Network Monitor (formerly the Passive Vulnerability Scanner) which is provided by DISA to DOD Customers at no cost. DISA’s Cyber Development (CD) provides program management for the Enterprise ACAS offering as well as help desk support and training.

**BOOTABLE MEDIA (BOOTME)**

Bootable Media (BootMe) is a lightweight live CD that temporarily creates a secure, non-persistent end node on almost any personal or public computer for safer, deployable, very-low-cost NIPRNet remote desktop access.

The product is designed to provide a secure virtual trusted bootable solution for remote access to DOD Information Networks (DODIN) enterprise services using non-Government Furnished Equipment (GFE) from home for telework, pandemic and continuity of operations (COOP).

**CYBERSECURITY SERVICE PROVIDER (CSSP)**

Provide Network assurance functions for the DISA enterprise, combatant commands (COMCOS), and DOD agencies that subscribe to DISA as their Cybersecurity Service Provider (CSSP).

Provide mission partner incident monitoring, detection with strategic vulnerability analysis and recommend CND response actions.

**ACROPOLIS**

Acropolis contains computer network defense - data monitored from DOD enterprise services, NIPRNet Internet access boundary monitoring, and SIPRNet secret provider edge routers.

This data combined with the Acropolis analysis and workflow suite of tools provides situational awareness of these computer networks used by the Department of Defense.

**CONTINUOUS MONITORING AND RISK SCORING (CMRS)**

Continuous Monitoring and Risk Scoring (CMRS) is a web based system that visualizes the cybersecurity risk of the Department of Defense (DOD) based on published asset inventory and compliance data. CMRS supports the risk management approach to cybersecurity oversight by quantitatively displaying an organization’s security posture through the use of risk dashboards.

Using the risk dashboards, users can gather actionable direction, implement prioritized mitigation decisions, and ensure effectiveness of security controls in order to support their cybersecurity risk management duties.

The DOD Endpoint Security Solutions (ESS) are an integrated set of capabilities that work together to detect, deter, protect, and report on cyber threats across all DOD networks. Endpoint security is a DOD-wide effort that leverages the collaborative capabilities of the National Security Agency, services, DOD CYBER Range, DOD’s Red Team support, and continuous market research through these DOD agencies.

The endpoint ecosystem includes integrated solutions such as Comply to Connect (C2C), containment, visibility, and assessment tools. The endpoint ecosystem is constantly reviewed via the NIPRNet/SIPRNet Cyber Security Architecture Review (NSCSAR) process to ensure appropriate protections are in place to meet the ever-changing threat.
THE GLOBAL GRAY NETWORK PILOT

The Defense Information System Agency has adapted the National Security Agency’s dual-encrypted virtual private network tunnels to provide secure connectivity. The Global Gray Gateway is a Commercial Solution for Classified (CSfC), managed by secure certificates and offered as an enterprise gateway service. This gateway infrastructure has a centralized certificate and network management function that enables thousands of projects/capabilities with the ability to use multiple CSfC capability packages for transit across the gateway.

• Classified data can be read anywhere using encryption technology to help traverse any unclassified, internet, or non-DOD network.
• The gray network is physically and logically under the control of the solution owner or a trusted third party.
• The gray network exists as a network between an inner virtual private network gateway and wireless local area network access system which contains single encrypted classified data.
• All information is afforded two layers of protection.

Content Delivery
Global Content Delivery Service (GCDS) provides commercial Internet technology to accelerate and secure DOD web content and applications across the Non-secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet) 24x7.

Data Services
Provide best effort IP-based services across the DOD enterprise based on the classification level of the information accessible, including sensitive but unclassified (SBU), secret (S) and top secret/sensitive compartmented information (TS/SCI).

Messaging Services
Messaging Services provide the ability to exchange official information between military organizations and to support interoperability with allied nations, non-DOD activities, and the intelligence community operating in both the strategic/fixed-base and the tactical/deployed environments.

Satellite Communications (SATCOM)
SATCOM services, combined with Commercial Satellite Communications (COMSATCOM) leases, allow worldwide access to Defense Information Systems Network (DISN) voice, data, video, and transport services.

Dedicated Transport
This capability delivers a private-line-transport service that provides point-to-point connectivity to mission partner locations.

Voice Services
DISA Voice Services provide reliable, secure and non-secure, high-quality voice and voice messaging services.

Virtual Private Network
Virtual Private Network (VPN) provides mission partners the ability to connect to the DOD network through various means and modes.
JOINT INTEROPERABILITY TEST COMMAND

JITC is DOD’s Joint Interoperability Certifier and only non-Service Operational Test Agency (OTA) for IT/National Security Systems. JITC provides risk based test, evaluation and certification services, tools, and environments to ensure joint warfighting IT capabilities are interoperable and support mission needs.

Joint Interoperability Certifier

Throughout the acquisition process, JITC assists in identifying joint interoperability requirements, and ensures interoperability is built into the system from the start. JITC aides in the most efficient use of resources, and also assists in identifying solutions to interoperability problems necessary to get the system certified.

Operational Test Agency

As an Operational Test Agency (OTA), JITC is responsible for planning and conducting operational tests, reporting results, and providing an evaluation of each tested system’s operational effectiveness, suitability, interoperability, and security. JITC is the OTA for IT and National Security Systems (NSS) acquired by the Defense Information Systems Agency, other Department of Defense (DOD) organizations, and non-DOD entities.

Warfighter Joint and Coalition Interoperability Support

JITC provides direct technical and regulatory interoperability support to the combatant commanders, services, and DOD agencies (CSAs) during the planning and execution of joint/combined operations and exercises in order to identify and resolve emerging and systemic interoperability issues.

JITC also maintains 24/7 hotline support to help resolve immediate warfighter interoperability issues. JITC’s hotline service is usually available at no cost to the military services, government agencies, and government sponsored contractors.

Major Range Test Facility

JITC is the only non-service Major Range Test Facility Base, servicing the DOD. As such, JITC is considered a national asset. Services that are provided include test and evaluation (T&E) capabilities, infrastructure, and resources to support the DOD acquisition system.

JITC Labs

JITC provides a wide array of labs focusing on the interoperability of communications systems, routers, Public Key Infrastructure (PKI) certificates, satellites, and waveforms to name a few.

JITC Labs support the warfighter by supporting a number of core functions within their respective areas of focus. Support includes emulating command environments, ensuring conformance to standards, and testing, evaluation, and certification of systems.
DOD Mobility provides enterprise-level classified and unclassified mobile communication services that ensure interoperability, increased security, access to information, and reliable service to the mobile workforce.

These service offerings are composed of secure networking and gateway infrastructure that provides and extends enterprise services (such as, email, voice, video) to mobile devices; an enterprise Mobile Device Management (MDM) system that provides application layer confidentiality, integrity, and authenticity; and an enterprise Mobile Application Storefront (MAS) that hosts mobile applications.

DOD Mobility Classified Capability (DMCC) is an enterprise service providing classified mobile access to the Secret Internet Protocol Router Network (SIPRNet). DMCC devices are portals to the classified networks; there is no data at rest. DMCC leverages commercial technology and products to the greatest extent possible while allowing access to SIPRNet email and secure voice communications via a secure Voice over Internet Protocol (VoIP) capability.

DISA Mobility is developing top secret-collateral mobile capability, voice only. This will allow calls to both TS/SCI phones connected to the Defense Red Switch Network (DRSN) and other DMCC-TS users.

DOD Mobility Unclassified Capability (DMUC) is an enterprise service that allows government purchased commercial mobile devices (CMD) access to the Department of Defense Information Network (DODIN), Defense Enterprise Email (DEE), and chat encrypted email capability, as well as access to hundreds of approved Apple and Android apps (commercial & government off the shelf).

DMUC leverages the latest commercial technology from industry carriers that support iOS, Android and Windows operating systems. This infrastructure allows broad access to enterprise services like Defense Enterprise Email (DEE) and provides a seamless user experience between desktop and mobile environments.

The Mobile Application Store (MAS) is an online digital electronic software distribution system that allows DMUC users to browse and download approved apps for their Apple or Android commercial mobile devices (CMD). Applications undergo in-depth vetting and analysis, and are mapped to various security requirements before they are made available at the Mobile Application Store (MAS). DISA has more than 200 approved apps available in the DMUC Mobile Application Store (MAS).

Purebred was developed by Public Key Infrastructure (PKI) Engineering and provides over-the-air (OTA) certificate credentialing capability to enable DOD personnel to use DOD PKI credentials on mobile devices. Purebred builds upon the success of the iOS software certificate pilot to provide an enterprise-grade solution and will also replace the need for any smart card reader (SCR) solutions for S/MIME and secure browsing. Purebred is an optional, add-on solution for DMUC customers.

The DMUC implementation allows users to:
- Send digitally signed and encrypted email.
- Decrypt encrypted email.
- Client authentication to supported DOD websites.
REFORM THE AGENCY
ENCORE III

ENCORE III is a multiple award, indefinite delivery, indefinite quantity (IDIQ) contract that provides IT solutions for activities throughout all operating levels of all customer organizations in support of functional requirements including command and control (C2), intelligence, and mission support areas, and to all elements of the Joint Information Environment (JIE).

Encore has been DISA’s primary vehicle for buying a wide range of IT services. It has 19 performance areas such as enterprise IT planning and policy, business process re-engineering, network support, and cloud professional services.

The contract has a five-year base and five one-year options.

SETI is a new multiple-award task order contract (MATOC) vehicle for the Department of Defense (DOD). It is based on innovation as a priority to solve the complex IT engineering and developmental requirements for DISA and its mission partners. SETI will consolidate and streamline critical engineering expertise to research, design, develop, implement, integrate, and optimize DOD IT capabilities, systems, and solutions.

SETI will provide an overarching, streamlined, and efficient procurement approach for ordering a variety of critical end-to-end engineering performance-based services while ensuring maximum opportunity for competition among SETI’s prequalified pool of innovative contractors from small and large business categories.

SETI’s main focus is on fostering, developing, and encouraging innovation with the goal to reduce costs, timelines, and provide innovative solutions to deliver capable, reliable, and consistent products/services to our nation’s warfighters.

Simultaneously, SETI searches for breakthroughs, efficiencies, and advancements performed in engineering technical solutions that have resulted in a significant decrease in cost/schedule and an optimization in performance — all while effectively managing the increased risk profiles that are inherent in solving complex capability gaps.

SETI’s pre-qualified pool of contractors will be continuously encouraged to think about, and propose, innovative approaches to deliver and develop more agile, cost-effective, and smarter solutions, systems, capabilities, and services to meet the evolving needs of the warfighter.
TRUSTED RELATIONSHIPS
WITH MISSION PARTNERS

DISA U.S. Africa Command Field Office
Mohringen, Stuttgart Germany
011-49 711-729-5602 / DSN 314-421-5602

DISA U.S. Central Command Field Command
MacDill AFB, Florida
(813) 529-6600 / DSN 312-529-6600

DISA U.S. European Command Field Command
Vaihingen, Stuttgart Germany
011-49-711-68639-5190 / DSN 324-434-5190

DISA Global Operations Command
Scott AFB, Illinois
(618) 418-8840 / DSN 312-418-8840

DISA U.S. Northern Command Field Office
Peterson AFB, Colorado
(719) 554-3800 / DSN 312-692-3800

DISA U.S. Indo-Pacific Command Field Command
Joint Base Pearl Harbor-Hickam, Hawaii
(808) 472-0051 / DSN 315-472-0051

DISA U.S. Special Operations Command Field Office
MacDill AFB, Florida
(813) 826-2086 / DSN 312-299-2086

DISA U.S. Southern Command Field Office
Doral, Florida
(305) 437-1666 / DSN 312-567-1666

DISA U.S. Strategic Command Field Office
Offutt AFB, Nebraska
(402) 294-5761 / DSN 312-271-5761

DISA U.S. Transportation Command Field Office
Scott AFB, Illinois
(618) 220-4074 / DSN 312-770-4074

DISA Joint Staff Support Center
Pentagon, Washington DC
(703) 697-7416 / DSN 225-277-7416

The following defense and federal agencies should contact:
disa.meade.bd.mbx.bdm1-agency-federal@mail.mil

- Department of Defense (DOD) Offices and Agencies
- Office of the Secretary of Defense (OSD)
- Federal Agencies
- U.S. Coast Guard (USCG)
- Intelligence Community

UNIFORMED SERVICES AND COMMANDS
disa.meade.bd.mbx.bdm2-ccmd-services@mail.mil

- Combatant Commands (CCMD)
- Joint Staff
- Military Services
  ◊ U.S. Air Force (USAF)
  ◊ U.S. Army (USA)
  ◊ U.S. Marine Corps (USMC)
  ◊ U.S. Navy (USN)

INTERNATIONAL RELATIONS & ENGAGEMENTS
disa.meade.bd.mbx.bdm3-international@mail.mil

GENERAL MISSION PARTNER SUPPORT
disa.meade.bd.mbx.bdm4-mpeo-support@mail.mil
Purchasing telecommunications and information technology (IT) products and services for the military is one of DISA’s key roles within the DOD.

Our contracting and procurement experts use a variety of contract vehicles to increase acquisition speed, reduce costs, and ensure the men and women of our armed services have the cutting-edge services and capabilities they need to fulfill their missions.

(301) 225-4120, DSN 375
Procurement Directorate/Defense Information Technology Contracting Organization (DITCO)
http://www.disa.mil/Mission-Support/Contracting

Small Business Advocacy enables DISA to gain access to the efficiency, innovation, and creativity offered by small businesses. We are an integral player and value-added advisor in the development of agency acquisition strategies to ensure compliance with laws, directives, goals, and objectives related to small business initiatives.

Headquarters Office: 301-225-6003
Satellite Office: 618-229-9667
Office of Small Business Programs

Vision: Optimize how DISA and Industry communicate.

Mission: Facilitate and foster mutually beneficial relationships with DISA’s industry partners.

Corporate Connections’ Role:

• Formulate DISA’s industry engagement strategy.
• Improve DISA’s visibility of agency-wide industry interactions.
• Build relationships with industry.

http://disa.mil/About/Industry-Partners