

DISA JFHQ DODIN CAPABILITIES

2019

CONNECTING AND PROTECTING THE WARFIGHTER IN CYBERSPACE



TRUST IN DISA: MISSION FIRST, PEOPLE ALWAYS

DISA JFHQ DODIN



DEFENSE INFORMATION SYSTEMS AGENCY

MISSION To conduct DODIN operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation.

JOINT FORCE HEADQUARTERS – DOD INFORMATION NETWORK

MISSION Exercise Global Command and Control of DOD Information Network Operations and DCO-IDM in order to synchronize the protection of DOD component capabilities to enable power projection and freedom of action across all warfighting domains.

STRATEGIC EFFORT

OPERATE AND DEFEND

ADOPT, BUY, AND CREATE SOLUTIONS

ENABLE PEOPLE AND REFORM THE AGENCY





OPERATE & DEFEND

JOINT FORCE HEADQUARTERS–DOD INFORMATION NETWORK (JFHQ-DODIN)

The shield of DOD cyberspace warfighting, enabling the defense of the Nation.



ABOUT JFHQ-DODIN

JFHQ-DODIN, a component command of U.S. Cyber Command, is responsible for securing, operating and defending the Department of Defense complex infrastructure of roughly 15,000 networks with 3 million users. JFHQ-DODIN leads unified actions across all DOD for DODIN operations and defeats, denies and disrupts cyber-attacks against the DODIN.

Through proactive actions in support of the National Defense Strategy and DOD Cyber Strategy, the Command works to reduce risks, vulnerabilities and threats to DOD missions, assets and information. This warfighter ethos and mindset reflects an essential shift from viewing information technology as administrative to leveraging the DODIN for operational gains across all core department functions—combatant command warfighting; the services' organize/man/train/equip functions; intelligence functions and business operations.

JFHQ-DODIN's unique role centers on command and control across DOD's 43 components with areas of operation on the DODIN terrain bringing value to their:

- operational effectiveness and mission assurance
- readiness for cyberspace operations
- ability to integrate cyber with other operational domain actions and regional efforts
- efforts to strengthen partnerships to combat cyberspace adversaries



KEY ASPECTS INCLUDE

Cyber Tasking Cycle & Priorities. The DODIN Cyber Tasking Cycle provides daily directives to the 43 components for defensive actions and system changes, sharing cyber-related information and intelligence with all DOD organizations and partners, interacting with operations center directors, and engaging with DOD commanders and directors to identify collective defensive cyber-related priorities. This work supports USCYBERCOM's full-spectrum persistent engagement strategy.

Fight the DODIN. Fight the DODIN—a 26-point strategic campaign approach to network operations, cybersecurity and defensive cyber actions at all levels—strengthens DOD's ability to have competitive advantage over adversaries. It is broken into five lines of effort:

Organize – all terrain is identified as part of an area of operation and assigned to a commander/director

Secure – terrain is secure across internet access points, passage lanes and boundaries

Operate – priorities guide decisions and defensive cyberspace operations are de-conflicted

Defend – terrain is defended in a proactive unified effort

Partner – partnerships with DOD organizations, other federal agencies coalition/international partners, and others reinforce effective results

Evaluating Risk-to-Mission. Looking Beyond Compliance. JFHQ-DODIN is implementing a Next Generation inspection initiative that builds upon the compliance-based Command Cyber Readiness Inspection program by increasing standards and incorporating a mission-based, threat-focused approach. This Command Cyber Operational Readiness Inspection integrates threat environment information along with a review of technology and process conditions to help commanders and directors understand the overall threats and vulnerabilities that impact their organization's ability to succeed with carrying out its mission objectives.

Standards, Requirements & Capabilities. JFHQ-DODIN bridges defensive cyber capability requirements and resourcing efforts to address both operational effectiveness and efficiency opportunities. Grounded in the operational command framework of the 43 DODIN areas of operations with JFHQ-DODIN's Directive Authority for Cyberspace Operations (DACO), JFHQ-DODIN works to develop performance standards, identify defensive cyber capabilities, optimize current capabilities, and operationalize modernization efforts and new technology solutions to improve speed, precision and agility in combating cyber threats and attacks.

To address critical operational initiatives, JFHQ-DODIN is leading matrixed, cross-functional task forces with DOD stakeholders to improve and standardize:

- Endpoint security
- Perimeter security
- Mid-point security
- Cross domain solutions
- Big data analytics
- Shared situational awareness
- Cloud-based architecture

UNDERSTANDING THE DODIN The DODIN is DOD's classified and unclassified complex federation of thousands of networks, information technology equipment, tools and applications, weapon system technologies and data. This includes mobile devices, Internet access points and connections with nonmilitary entities, platform information technology, programs of record, industrial control systems/supervisory control and data acquisition, and the cloud environment.

The DODIN is composed of service, agency and combatant command constructed networks. It encompasses the enterprise, and the base, post, camp and station levels. The Defense Information Systems Network (DISN), managed by DISA, serves as the DODIN backbone.

COMPUTING

THE DISA COMPUTING ECOSYSTEM

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.

COMPUTING LINES OF BUSINESS

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.

OPERATIONS

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

The DISA Command Center (DCC) exercises the authority of the DISA director to command and control, operate, and defend DISA's portion of the DODIN. The DCC is the operational synchronization center of DISA, operating a 24x7 watch floor and continuously assessing the overall health of DISA's infrastructure and services enabling persistent and assured global services across the enterprise.

The DCC is the central point for providing enterprise level situational awareness (SA) for operation and defense of all DISA services to senior leadership of DISA and the DOD.

The DCC issues orders and directives to effect change in DISA's environment. In the event of conflicting operational priorities between any DISA operational elements, the DCC serves as the final adjudication authority

Defensive Cyber Operations (DCO):

DISA's DCO division plans, synchronizes and directs the security and defense of DISA's portion of the DODIN. It also directs the agency's defensive cyberspace operations-internal defense measures (DCO-IDM) to support the DOD mission.

Three Functional Areas:

- DCO Current Operations: performs defensive cyber activities related to day-to-day protection of the DISN.
- DCO Strategy, Plans and Transformation: provides a governance and strategic structure that enables synchronization across the DCO community.
- Cybersecurity Service Provider (CSSP): provides the programmatic activities of DISA's CSSP program

INFRASTRUCTURE

DISA implements and sustains the global network infrastructure in order to provide information superiority to the President, Combatant Commanders, senior leadership, military services, agencies, and the warfighter. Through the agency's Infrastructure Directorate, DISA provides world-class DOD Information Network (DODIN) core infrastructure and capabilities for mission partners by sustaining and optimizing the Defense Information System Network (DISN) infrastructure at approximately 3,500 locations in 26 nations. The organization also manages terrestrial and undersea transport, satellite, mobile gateways and multinational information systems.

Transport

Provides transport systems to support the enterprise infrastructure that allows the warfighter the power to connect to information resources globally.

Satellite Communications (SATCOM)

Delivers global, reliable, and resilient services while continuously improving the capabilities of satellite communications.

Communications Gateway

Implements and sustains the communications gateway infrastructure and sustains the DOD Organizational Messaging Service (OMS) for automated messaging between combatant commands, services and agencies using global addressing and routing via the National Gateway Centers (NGC).

Implementation and Installation

Manages DISN telecommunications release activities and oversees worldwide deployment for all corresponding services and associated logistical support. This function provides critical circuit provisioning, installation, project control, and task order management activities in direct support of the sustainment and maintenance of the DISN and its warfighter customers.

Communications Engineering

Provides world-class engineering support for the DISA, DISA programs, DOD strategic communications and SATCOM while serving as the primary source of end-to-end communications engineering expertise for DISA and DOD.

Special Services

Provides requirements analysis, services, and communications support at the speed of technology for the DISN, the United States Secret Service, and Joint Staff Office of Special Events; manages the global internet for the classified and unclassified internet protocol (IP) addressing; and provides circuit provisioning, project control, and other activities in direct support of the telecommunication needs of the warfighter.

SERVICE AND SUPPORT

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.**

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 battlespace 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.

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.

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.

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 SOLUTIONS.



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).

CLOUD STORAGE

Cloud storage is a portfolio of two cloud based storage offerings: milDrive and Storage as a Service (STaaS).

- milDrive – a personal file store with collaboration and flexibility in mind. Allows synchronization of files between local drive and cloud, allowing customers to share files. milDrive leverages security controls to provide least privilege.
- Storage as a Service (STaaS) – provides bulk storage for applications, backups, or system images. Organizations interested in backing up images of their virtual machines would have the ability to manage their own backup and restore of systems using this solution

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)

Defense Enterprise Office Solutions (DEOS) is a DOD-wide single enterprise solution for common communication, collaboration and productivity. DEOS will be mission effective, secure, cost-effective, efficient, ubiquitously accessible, intuitive and enable DOD to operate and fight worldwide.

DEOS supports the department-wide need for greater functionality and efficiency. By leveraging joint collaboration capabilities DEOS strengthens the DOD cybersecurity posture and creates a simpler, defensible perimeter by reducing DOD's footprint. In addition, this enterprise solution, which leverages proven commercial capabilities, will support tactical environments.

DOD has partnered with the General Services Administration (GSA) to issue a DOD-wide GSA Schedule 70 Blanket Purchase Agreement (BPA) for DEOS.

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.



Desktop-based GVS

An enterprise-grade service that provides VTC capabilities to users from their desktop.

Note

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

ENTERPRISE VOICE OVER INTERNET PROTOCOL (EVOIP) ENTERPRISE CLASSIFIED VOICE OVER INTERNET PROTOCOL (ECVOIP)

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 46-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.



GCCS-JE

GLOBAL COMMAND AND CONTROL SYSTEM-JOINT ENTERPRISE

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.

C2 PORTFOLIO

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.



CYBERSECURITY

JOINT REGIONAL SECURITY STACKS

The Joint Regional Security Stacks (JRSS) is a joint cyber warfighting platform consisting of network security capabilities that provides enhanced network command and control which allows DOD to continuously monitor and evaluate data routed through the DODIN.

JRSS provides this capability through standardized, regionally focused, physical infrastructure known as “stacks” that allow DOD to intake and rapidly transport large sets of data.

The JRSS management tools enable network defenders and defensive cyber operators to see, manage and assess data passing through the stacks to maintain situational awareness of systems and ensure response time and manage data quantity and performance standards.

JRSS is now centralizing the department’s network security into regional architectures, instead of locally distributed architectures at each military base, post, camp, or station to deliver a more secure, defensible and responsive Department of Defense integrated network, providing enhanced command and control capability. Essentially, JRSS reduces the cyber-attack surface and reduces cost for implementing and sustaining this capability for the entire DOD.

JRSS reduces the number of enemy attack vectors to the DODIN by consolidating multiple security gateways into single access points to the DODIN. Reducing the number of security gateways provides fewer opportunities for a hacker to access the DODIN.



PERIMETER DEFENSE

Through the development and deployment of boundary, or perimeter, defense capabilities DISA protects the DODIN from web and email threats posted by connections to the internet.

Perimeter capabilities that secure DOD networks at their point of contact with the internet and other external networks include:

- Enterprise Email Security Gateway (EEMSG)
- Zero-day Network Defense (ZND)
- Sharkseer
- Enterprise Break and Inspection
- Web Content Filter
- Distributed Denial of Service
- Domain Name System Hardening (DNS)
- NIPRNet Demilitarized Zone (N-DMZ)
- NIPRNet Federated Gateway Security



ENDPOINT SECURITY

ANTI-VIRUS/ANTI-SPYWARE SOLUTIONS

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.

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.

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 (COCOMS), 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.

ENTERPRISE COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) GATEWAY CONVERGENCE - UNIVERSAL DODIN GATEWAY

The Universal Gateway will consist of all enterprise infrastructure required to support terrestrial, mobile and satellite communications services (voice, video and data) to all DODIN customers worldwide. Numerous, existing discrete gateways (e.g. DOD Mobility Classified Capability, DOD Enterprise Classified Travel Kit, etc.) will be converged into a single gateway architecture incorporating new Commercial Solutions for Classified (CSfC) capabilities while continuing to support traditional encryption methods using Type 1 hardware. The Universal Gateway will provide all required gateway functions at all layers of the OSI stack for all communications entering or exiting the DODIN regardless of whose it is, what it is, where it is going or how it is getting there.

- CSfC is used in several existing DISA-provided systems and represents the future of encryption for everyday classified mobile and transportable communications.
- DISA’s goal is to fully support emerging CSfC capabilities as well as traditional encryption methods via all transport mechanisms.
- DISA is currently converging several discrete gateways and will soon field the first consolidated system.

Enterprise CSfC will allow mission partners greater connectivity to classified networks by using commercial-grade encryption technology to securely traverse any unclassified, internet, or non-DOD network



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.



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.



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.

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.

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 PROGRAM

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.



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.

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 APPLICATIONS

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).

DOD MOBILITY CLASSIFIED CAPABILITY - SECRET AND TOP SECRET

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

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).



DERIVED CREDENTIALS/PUREBRED

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.

EMERGING TECHNOLOGY

TECHNOLOGY INITIATIVES

Assured Identity: Increase assurance and protection of the warfighter's identity using their mobile device.

Artificial Intelligence (AI): Using the latest advances in AI to drive automation efficiencies, reduce manual support requirements and offer cost savings to our customers and system owners.

Cloud Based Internet Isolation: Reduce attack surfaces with the exponential DOD internet traffic growth by moving to isolated cloud-based platform.

Desktop Replacement: Desktop replacement for your phone by displaying a desktop-like environment to a monitor using a dock and connected wireless or wired peripherals.

Mobile Container Customization: Customization of mobile containers that allows other identity factors to unlock a secure workspace while enabling continuous multifactor authentication (CMFA).

Mobile Hardware Protection: Increasing mobile device physical hardware while maintaining functionality and avoiding security risks.

Personalized Contextual Authentication: Continuously authenticate a warfighter's identity by monitoring behavioral factors on how they interact with their device.

TECHNOLOGY ACCELERATORS

Cooperative Research and Development Agreements (CRADAs): Non-procurement agreements between DISA and external entities that allow parties to exchange personnel, facilities, equipment, services, and other resources to accomplish research, development, testing and evaluation (RDT&E) efforts consistent with the agency's mission and transfer technologies to the commercial marketplace.

Technical Exchange Meetings (TEMs): Cohosted by DISA and the DOD Chief Information Officer, these meetings invite industry leaders and academia to present emerging technologies beneficial to DOD and other federal agencies. Invitations to participate are extended across DOD and the Federal government.

Lean Startup Training: An approach to creating and managing innovation efforts to get a desired product into customers' hands faster.

DISA-Ruptive: Transforms innovative ideas submitted by DISA employees into new business processes, services, and technologies.

LEVERAGING RAPID ACQUISITION

Other Transaction Authorities (OTAs): Offer a streamlined method for carrying out prototype projects and transitioning successes into follow-on production.

Commercial Solution Openings (CSOs): Provide a streamlined approach for acquiring innovative commercial items.

Rapid Innovation Fund (RIF): Designed to fund mature prototypes and technology ideas.







ENABLE PEOPLE AND REFORM THE AGENCY

CONTRACTING

SYSTEMS ENGINEERING, TECHNOLOGY, AND INNOVATION (SETI)



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.



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.

ENABLE PEOPLE

QUALITY OF WORK LIFE

DISA is committed to fostering an environment that not only responds to the various needs and goals of its employees, but is also conducive to a better quality of life in general. DISA achieves this through a variety of programs designed to promote a more beneficial lifestyle both professionally and personally.

- Compressed Work Schedule
- Employee Assistance Program
- Mass Transit Subsidy
- Worklife4U Program
- Telework Program
- Wellness Program



HIRING PROGRAMS

DISA Pathways Programs

- **Internship Program**

This Program is designed to provide students enrolled in a wide variety of educational institutions, from high school to graduate level, with opportunities to work in agencies and explore Federal careers while still in school and while getting paid for the work performed. Students who successfully complete the program may be eligible for conversion to a permanent job in the civil service.

- **Recent Graduates Program**

This program is for individuals who have recently graduated from qualifying educational institutions or programs and seek a dynamic, career development program with training and mentorship. Successful applicants are placed in a dynamic, developmental program with the potential to lead to a civil service career in the Federal Government.

Aspiring Leaders

- **Schedule “A” Appointments**

The Schedule “A” authority is for all people with disabilities. This authority is used, at the agency’s discretion, to appoint candidates to any grade level for any job (time-limited or permanent) for which they qualify.

- **Veterans’ Preference**

Gives eligible veterans preference in many appointments over other applicants and applies to virtually all new appointments in both the competitive and excepted service.

- **Veterans’ Recruitment Appointment (VRA)**

An excepted authority that allows agencies to appoint eligible veterans without competition at any grade level up to and including a GS-11 or equivalent. This is an expected service appointment.

- **Veterans Employment Opportunity Act (VEOA)**

A competitive service appointing authority that can only be used when filling permanent, competitive service positions (not excepted service positions). It allows veterans to apply to announcements that are only open to “status” candidates, which means “current competitive service employees.”

TRAINING PROGRAMS

DISA helps employees to reach their professional goals through a wealth of leadership training and educational initiatives to maximize career development.

- Competitive Development Programs
- Leadership Programs
- Professional Licenses and Certification Programs
- Leadership and Technical Speaker’s Forum
- DISA eLearning



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

MISSION PARTNER ENGAGEMENT OFFICE

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

TRUSTED RELATIONSHIPS WITH INDUSTRY PARTNERS

CONTRACTING OPPORTUNITIES

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

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

<http://www.disa.mil/Mission-Support/Small-Business>

OFFICE OF STRATEGIC COMMUNICATION & PUBLIC AFFAIRS: CORPORATE CONNECTIONS

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>

DISA
JFHQ DODIN