

Defense Information Systems Agency

DISA Enterprise Business Service Catalog

This catalog represents DISA's initial effort to present services available through the agency. At this time, only Computing Services, Network Services, and the Field Security Office services are included. A more comprehensive catalog is under development and will be incorporated on our website and released in the coming months.

Release 1, Version 1.1
19 October 2011

UNCLASSIFIED



This page intentionally left blank.

REVISION HISTORY

Date	Version Number	Section Reference	Changed By:	Description
9/28/11	1.0	ALL	Computing Services	Document Release 1
10/19/11	1.1	Cover Page	Catalog Manager, CSD	Document release 1

POINT OF CONTACT

For questions regarding this document, please contact the Service Catalog Manager.

Contact	Contact Information
Service Catalog Manager Phone	CML: 303-224-1768 DSN: 926-1768
Service Catalog Manager E-Mail	CSD_SLM@csd.disa.mil

TABLE OF CONTENTS

INTRODUCTION.....	1
1. AUTOMATED TIME, ATTENDANCE, AND PRODUCTION SYSTEM.....	3
2. CAPABILITY IMPLEMENTATION.....	4
3. COMMERCIAL SATELLITE SERVICE.....	5
4. COMPLIANCE INSPECTIONS.....	6
5. CONTINUITY OF OPERATIONS/SERVICE CONTINUITY.....	8
6. DATA COMMUNICATIONS.....	10
7. DEDICATED SERVICE	13
8. DIAL-UP AND DEDICATED VIDEOCONFERENCING.....	14
9. DOD ENTERPRISE E-MAIL.....	16
10. ENHANCED MOBILE SATELLITE SERVICES.....	18
11. ENTERPRISE SHAREPOINT SERVICE	20
12. FORGE.MIL	21
13. GLOBAL CONTENT DELIVERY SERVICE	22
14. IBM MAINFRAME APPLICATION HOSTING.....	25
15. IBM MAINFRAME Z/LINUX APPLICATION HOSTING	26
16. INFORMATION ASSURANCE STANDARDS AND TRAINING.....	28

17.	INTERNATIONAL MARITIME SATELLITE.....	29
18.	MULTILEVEL SECURE VOICE.....	31
19.	NETWORK DEFENSE.....	33
20.	ORGANIZATIONAL MESSAGING SERVICE.....	35
21.	RAPID ACCESS COMPUTING ENVIRONMENT	36
22.	SECRET INTERNET PROTOCOL DATA	37
23.	SECRET TEST AND EVALUATION INTERNET PROTOCOL DATA.....	39
24.	SECURE FILE GATEWAY RELAY SERVICE	41
25.	SECURE MOBILE ENVIRONMENT PORTABLE ELECTRONIC DEVICE	42
26.	SENSITIVE BUT UNCLASSIFIED INTERNET PROTOCOL DATA	43
27.	SENSITIVE BUT UNCLASSIFIED VOICE	45
28.	SERVER APPLICATION HOSTING.....	46
29.	STORAGE SUPPORT FOR SERVER-BASED APPLICATIONS.....	48
30.	SYSTEM NETWORK AVAILABILITY PERFORMANCE SYSTEM	51
31.	TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION INTERNET PROTOCOL DATA	52
32.	TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION VIDEOCONFERENCING.....	53
33.	TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION VOICE.....	54
34.	UNISYS MAINFRAME APPLICATION HOSTING.....	55



35. VOICE AND CIRCUIT SUPPORT 56

36. VOICE OVER SECURE INTERNET PROTOCOL 58

37. WEB HOSTING..... 59

APPENDIX A – ACRONYMS A-1

APPENDIX B – REFERENCES AND CITATIONS B-1

INTRODUCTION

The Defense Information Systems Agency (DISA) Enterprise Business Service Catalog (E-BSC) provides a description of the services we offer our mission partners, as well as the service features, options, costs, ordering procedures and support points of contact (POCs).

Purpose

The purpose of the E-BSC is to present our mission partners with a centralized resource of accurate information detailing the cloud computing, application hosting, information assurance, Defense Information System Network (DISN) telecommunications, and emerging services DISA offers. The E-BSC provides this information in a single, comprehensive source to ensure consistency of information to those authorized to access the catalog.

Scope

The scope of this catalog includes the Cloud, Computing (to include Application Hosting), DISN Telecommunications, and Information Assurance (IA) services DISA provides its mission partners. In addition, the emerging services are described – those services in the pipeline being rapidly developed but not yet ready as full production offerings. Additional/remaining DISA services not yet included in this E-BSC will be incorporated in the near future.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

DISA provides Computing services in response to our partners' operational requirements. Services are provided within a backdrop of world-class computing facilities located in both the continental United States (CONUS) and outside of the continental United States (OCONUS). DISA's mission is to deliver computing information products and services that enable and enhance the ability of our partners/end users to execute their missions. These services provide highly efficient and secure raised floor operations for hosting our partners' systems/applications.

The DISN is a worldwide-protected telecommunications network that enables the exchange of information in an interoperable and global space, partitioned by security demands, transmission requirements, and geographic needs of targeted mission partner communities. The DISN offers a selection of integrated standards-based services,



providing our mission partners with capability options that support their diverse telecommunications requirements.

DISA provides IA products and services in response to partner operational requirements. DISA's mission is to enhance security and availability of the GIG by developing and ensuring adherence to IA policies and guidelines.

DISA continues to research, design and deploy new service offerings which will bring higher levels of support to all Department of Defense (DoD) entities. An example of that is the advancement of Enterprise-Level Cloud Services to bring more efficient, effective and faster service to the warfighters and other end users.

1. AUTOMATED TIME, ATTENDANCE, AND PRODUCTION SYSTEM

The Automated Time, Attendance and Production System (ATAAPS) cloud service is a web-based application that provides an online facility for the entry, update, concurrence and certification of time and attendance data for civilian employees of various DoD agencies. It serves primarily as a data entry and repository system, which then feeds payroll data to the DoD payroll system. DISA provides our partners within the federal government with unique application and Service Desk support. DISA currently supports over 83,779 user accounts.

1.1 Features

This service provides labor and leave reporting and accountability. It directly interfaces with the Defense Finance and Accounting Service (DFAS) for payroll processing.

1.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

1.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the Service Level Agreement (SLA) which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling the Computing Services Directorate (CSD).

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

2. CAPABILITY IMPLEMENTATION

Capability Implementation consists of operationalizing IA products to ensure a smooth transition from the development process to an operational environment.

2.1 Features

Capability implementation features in support of IA material solutions about to be fielded.

- **Implementation** – The fielding and implementation of Computer Network Defense (CND) technologies into the operational environment to support Tier 2 and 3 CND Service Provider (CNDSP).
- **Configuration Management** – The configuration management processes associated with new and existing CND technologies utilized to support operations for Tier 2 and 3 CNDSP. Activities involve baseline maintenance, system administration, and vulnerability management.
- **Product Concept of Operations (CONOPs)/Tactics, Techniques, and Procedures (TTPs) Development** – The development of capability solutions with CONOPs solutions and supporting TTPs. These documents are developed for all roles including: users, operators, analysts, system administrators, etc.
- **Deployment, Implementation, Maturization & Effectiveness (DIME)** – Standard methodology and vendor services for gaining resource efficiencies and achieving full solution operationalization across DoD.
- **Vulnerability Management System (VMS) Operations** – VMS operations support current VMS partners and provide operationalization support to new and current VMS partners.

2.2 Rates

In Fiscal Year 2013, Field Security Operations (FSO) is proposed to become a Defense Working Capital Fund (DWCF) entity. As such, the cost of many services will be billed directly to service recipients based on an Office of the Secretary of Defense (OSD) Comptroller rate schedule.

Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

2.3 Additional Information

Additional service and ordering information can be found by emailing or calling FSO.

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO E-Mail	FSO_SLM@disa.mil

3. COMMERCIAL SATELLITE SERVICE

The Commercial Satellite Service (CSS) satellite service utilizes a number of different satellite services to provide warfighters with worldwide access and Global Information Grid (GIG) connectivity for diversity, redundancy and availability. DISA is the DoD's only authorized service provider for commercial fixed satellite services and serves as an advocate for the use of commercial satellite communications in order to increase the availability and flexibility of military communications.

CSS allows for the lease or acquisition of terminals, teleports, landlines, Operations and Maintenance (O&M) support, host-nation support and approvals (i.e., negotiation support services, host-nation approvals, landing rights, frequency clearance, terminal registration, licenses, authorization to operate the terminals), engineering and any other communications resource our partners may require, providing for a true end-to-end, turnkey solution.

Warfighters are provided with access to Sensitive but Unclassified (SBU) Internet Protocol (IP) Data, Secret IP Network Data, Top Secret/Secret Compartmented Information (TS/SCI) IP Data, SBU Voice and Multilevel Secure Voice to meet their voice and data requirements.

This service supports up to and including TS/SCI security classification.

3.1 Features

- Satellite Communications (SATCOM) gateway systems combined with Commercial SATCOM (COMSATCOM) leases allow worldwide access to DISN voice, data, video and transport services
- DoD gateways continually improve GIG connectivity, diversity and redundancy to increase availability and reliability

- IA upgrades protect gateway and partner systems and data

3.2 Rates

For assistance in obtaining CSS pricing, potential partners should refer to the CSB group website at: <http://www.disa.mil/satcom/ss1.html>.

3.3 Additional Information

Our mission partners order DISN telecommunication services via the DISA Direct Order Entry (DDOE) application located at <https://www.disadirect.disa.mil>.

For Commercial Satellite Service, the Global SATCOM Support Center (GSSC) is the single POC service support for all COMSATCOM mission partners. The GSSC operates 24 hours a day, 7 days a week, 365 days a year, and can be contacted as follows:

Organization	Contact Information
GSSC	CML: (719) 554-5531 DSN: (312) 693-5531
GSSC e-mail	GSSC@peterson.af.mil
Regional SATCOM Support Center (RSSC)	CML: (813) 828-6845 DSN: (312) 968-6845
RSSC e-mail	RSSC@macdill.af.mil

4. COMPLIANCE INSPECTIONS

Compliance Inspections consist of conducting formal certification reviews and supporting other aspects of the risk management process, conducting cyber readiness inspections on behalf of United States Cyber Command (USCYBERCOM), and coordinating Net Assurance activities across DISA and COCOMs.

4.1 Features

The features of this service included distinct inspections, reviews and assessments which FSO can provide to assure your IA integrity and compliance with DoD IA Certification and Accreditation Process (DIACAP) and other regulations.

- Command Cyber Readiness Inspection (CCRI) – A formal inspection conducted under the direction of USCYBERCOM’s Enhanced Inspection Program.

- Security Assistance Visits (SAVs) – A process by which DISA FSO personnel will conduct an on-site assessment and validation of compliance with mandated IA, CND, certification and accreditation (C&A), or other focus areas either as a standalone effort or in preparation for a scheduled inspection or evaluation.
- CNDSP Level II Inspections – CNDSP evaluations are an on-site evaluation and validation of compliance with mandated CND Service requirements as outlined in DoD O-8530.1 and DoDI O-8530.2.
- CNDSP Level II Designation Assessments – CNDSP validations are a review and validation of alignment to an accredited CNDSP. A formal recommendation is provided upon completion of the on-site evaluation.
- IA Readiness Reviews (IARRs) – A formal review in 12 IA areas to determine a site's current IA program status and provide formal recommendations for improvements in areas where deficiencies or non-compliance are discovered.
- Enclave and System Certification – Can provide on-site technical assessments and certifications recommendations to a Designated Approving Authority (DAA) in support of enclave accreditation, coalition enclave or systems.
- Combatant Command (COCOM) exercise support – FSO provides critical exercise support for the COCOMs in various theater and global exercises. This support can come from a variety of areas and include CND technology Subject Matter Experts (SMEs), CND Integrators, and CND analysts.

4.2 Rates

In Fiscal Year 2013, FSO is proposed to become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule.

Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

4.3 Additional Information

Additional service and ordering information can be found by emailing or calling FSO.

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO E-Mail	FSO_SLM@disa.mil

5. CONTINUITY OF OPERATIONS/SERVICE CONTINUITY

DISA provides regulatory-compliant remote recovery capability, or Continuity of Operations (COOP), for our partners who purchase that service and document the requirement within their governing SLA. The standards and minimum requirements outlined in DoD Instruction (DoDI) 8500.2 include continuity-related IA controls. Those minimums form the foundation for the program as administered by DISA.

5.1 Features

5.1.1 Standard Features

COOP/Service Continuity consists of the policies, procedures, and programs that allow DISA, in concert with partner personnel, to provide an effective level of assurance that workloads will continue to process in accordance with regulatory requirements and documented obligations in SLAs.

5.1.2 Optional Features

There are six options available for server-based COOP/Service Continuity – five standard options and an additional custom option.

The table below shows the five standard options known as Remote Recovery Combinations (RRCs). In order to have a recovery option that meets the COOP requirements detailed in DoDI 8500.2, appropriate selections must be made for both storage (data) recovery and server (processor) recovery.

Option	MAC Level	Description	Storage Offering	Processor Offering	RTO/RPO
RRC 1	MAC III	Remote recovery using tape-based data backups and shared processing capability at the default designated recovery site	Basic Remote	Shared COOP	Recovery Time Objective (RTO) = 5 Days Recovery Point Objective (RPO) = 7 Days
RRC 1.2	MAC III	Remote recovery using replication of data and shared processing capability at the default designated recovery site	Operational Remote	Shared COOP	RTO = 5 Days RPO = 24 Hours
RRC 2	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured processing capability at the designated recovery site	Operational Remote	Dedicated COOP	RTO & RPO = 24 Hours
RRC 3	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured processing capability at the designated recovery site	High-Availability Remote	Dedicated COOP	RTO & RPO = 8 Hours
RRC 4	MAC I	Remote recovery using near-synchronous replication of data as well as dedicated, pre-configured, and operational processing capability at the designated recovery site	Non-Disruptive Remote (Host-Based Replication Only)	Dedicated COOP	RTO = 30 Min RPO = 1 Sec

Custom (Option 6) is available to those where mission requirements for a particular application, or suite of applications, are not adequately addressed by any of the standard options identified above.

5.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

5.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

6. DATA COMMUNICATIONS

DISA has network monitoring tools at its disposal to provide outstanding service for our partners. DISA provides and maintains the GIG utilized by partners. Network operations support is provided by a 24x7 staff responsible for identifying and resolving network problems, upgrading network devices and change management. SBU IP and Secret IP Data network availability is built into the system via hardware and circuit diversity throughout the Wide Area Network (WAN).

DISA is responsible for separate enclaves used to support DECC connectivity and applications. The same degree of circuit and hardware redundancy is provided to support the same degree of survivability. DISA hosts DoD demilitarized zone (DMZ) access nodes and DoD DMZ extensions that provide our partners with the ability to secure their applications in accordance with the DoD DMZ Security Technical Implementation Guide (STIG).

6.1 Features

The communications component is comprised of the DISA internal communications infrastructure and support teams. This infrastructure allows end-users, anywhere in the world, to connect safely and securely to the data that resides within DISA's processing centers.

- Data Transmission Options

DISA will provide a variety of options to satisfy data transmission requirements to mitigate the potential risk with using unauthorized ports and protocols. These services are no longer billed to the partner. The following table describes each of the options.

Traffic Flow	Solution to Use	Notes
Site-to-site Virtual Private Networks (VPNs)	Varies	
.com → .mil (Defense Enterprise Computing Center [DECC])	Business to Business (B2B)	Complete B2B/VPN checklist and follow instructions enclosed.
.mil → .mil (DECC)	Policy-Based Co-Location (PB Collo)	If partner is collocated at DMZ, use partner VPN equipment. If partner is not collocated at DMZ, use DISA provided VPN. Complete B2B/VPN checklist and follow instructions enclosed.
.mil (DECC) → .mil (DECC)	Inter-DECC Virtual Routing and Forwarding (VRF)	No configuration needed
DISA has deployed proxies that are used for any .com or .mil → .mil (DECC) based on Ports, Protocols and Services Management (PPSM) and associated boundaries	DMZ Proxy	
Ports 20,21 – File Transport Protocol (FTP) (User initiated)	Mainframe Internet Access Portal (MIAP)	Complete MIAP application online at https://miap.csd.disa.mil

Traffic Flow	Solution to Use	Notes
Ports 20,21 – FTP (Batch initiated)	B2B or PB Collo & Global Exchange (GEX) (on the backside)	Complete B2B PB Collo checklist as well as the GEX checklist
Port 22 – Secure Shell (SSH)/Secure FTP (SFTP)	GEX	Complete GEX checklist
Port 23 – Telnet	MIAP	Complete MIAP application online at https://miap.csd.disa.mil
Port 25 – Email	Mail Relay Services	Complete Mail Relay checklist
Port 80 – Hypertext Transfer Protocol (HTTP)	Web Proxy	Complete Web DMZ checklist
Port 443 – HTTP Secure (HTTPS)/Secure Socket Layer (SSL)	Web Proxy	Complete Web DMZ checklist
Port 1414 – Message Queuing (MQ) Series	GEX	Complete GEX
.mil (DECC) → .com or .mil on Transmission Control Protocol (TCP) port 80 or 443	DMZ Forward Proxy	No configuration needed above DMZ VPN Router (top side of the Community of Interest Network [COIN])
Any .mil → .mil (DECC) that is not proxiable or is not required to be proxied based on PPSM and associated boundaries	DMZ Non-Proxy	Firewall (FW) rules need amended in Non Proxy context on DMZ FW for required ports.

The following communication services are included in the basic processor rates and the partner will not incur an additional charge.

- B2B Gateway/DMZ Non-Proxy Gateway
- Web DMZ

6.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

6.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

7. DEDICATED SERVICE

Dedicated Service is a private-line-transport service that provides point-to-point connectivity to our partner locations. This service supports up to and including TS/SCI security classification.

7.1 Features

- Ability to carry multiple classifications of traffic
- Small and constant latency per connection
- Efficient utilization of bandwidth
- Wide geographic deployment, which reduces leased-line distances and cost

7.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

7.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

The DGSC serves as the mission partner POC for Dedicated Service.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

8. DIAL-UP AND DEDICATED VIDEOCONFERENCING

The Dial-up and Dedicated Videoconferencing service is a “meet me” type of service to the DISN Video Service – Global (DVS-G) system and consequently depends on its users to have the appropriate infrastructure to access the system. Dial-up and Dedicated Videoconferencing services are available 24 hours a day, 7 days a week, 365 days a year to registered users using fixed, deployed-fixed and mobile resources. These services allow simultaneous video and audio communication between two or more videoconferencing facilities (VCFs). The video services include point-to-point and multipoint videoconferencing service between dial-up and dedicated VCFs at unclassified, secret and Allied secret security levels.

A dial-up mission partner can use any of the switched transmission services available (government or commercial).

A dedicated VCF uses a dedicated T1 circuit to connect to the nearest hub.

8.1 Features

DISN video service offers seven types of conferences, including the following:

- Tele-broadcast – Video and audio signals are sent from one VCF to two or more VCFs without a signal being sent in return. This is similar to watching a television broadcast.

- Tele-seminar – Video and audio signals are sent from one VCF to two or more VCFs and only the audio signal is returned. This allows for a fully interactive audio in the conference. This method is often used for distance learning because all participants can see the instructor and hear each other's questions or comments.
- Interactive – Video and audio signals are sent and received by all participants in the conference. This type of DISN Video Services multi-point conference can incorporate one of three different types of switching. Switching refers to the way the control of the conference is handled. DISN Video Service offers four modes of switching.
- Voice Activated – No individual is assigned overall control of the conference and the monitors will change to show the person currently talking.
- Lecture – The lecturer retains control of the conference. The lecturer may allow others to brief but will never relinquish control of the videoconference.
- Chairperson control – The current speaker is in control of the conference. When the current speaker has completed speaking, the speaker selects and passes control to the next speaker(s).

8.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

8.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for Dial-up and Dedicated Videoconferencing.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

9. DOD ENTERPRISE E-MAIL

NOTE: Currently being provisioned for selected Army users only

DISA provides a DoD Enterprise E-Mail Solution, a cloud service, to the warfighter that consolidates DoD corporate e-mail to fewer servers and server locations, centralizes all e-mail management department-wide, and greatly reduces the cost per seat of providing email service to consumers of the service. As a Managed Service Provider (MSP), DISA is responsible for managing and operating the storage and server hardware, Operating Environment (OE), core e-mail applications, networking equipment and data center DMZ security services necessary to create the connection between the Military Services, DoD Agencies, and DISA networks.

DISA manages all applications making up the service, but shares some management responsibility with consumer organizations with respect to mobile devices such as BlackBerry and WinMobile devices. DISA provides the full lifecycle service for applications, computing, storage, and network infrastructure, and associated Data Center and information security services in order to meet the common objectives of availability, scalability, security, and manageability for the DoD Enterprise Email Service.

9.1 Features

9.1.1 Standard Features

- System Administration
- Security
- Data Communications
- Enterprise System Management (ESM) Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/Information Technology (IT) Service Continuity

- Engineering
- Hardware & software tech refreshes
- Transparent upgrades as new versions are released
- High availability through auto-failover between pods and between DECCs
- Common Access Card (CAC) enabled Outlook Web Access (OWA) and Outlook client
- Mailbox location assigned geographically to provide best performing pod
- Mailbox sizes of four gigabyte (GB) (average) for thick client users and 500 kilobyte (KB) for web users
- Full Blackberry, SME-PED, and Windows Mobile support
- Shared Organization Calendars
- Enterprise Global Address List (GAL) with 4.5 million DoD CAC holders
- Enterprise e-mail address and Enterprise display name
- 24x7 Operations and GIG Global Infrastructure Service Management Center (GISMC) monitoring
- Full Network Operations (NetOps) and CNDSP support

9.1.2 Optional Features

- Business Class Users
 - Simple Mail Transfer Protocol (SMTP) to/from anywhere
 - OWA from anywhere
 - Outlook Anywhere (SBU IP only)
 - Blackberry
 - Windows Mobile
 - 4GB average mailbox size
- OWA Only Users
 - OWA from anywhere
 - 500 megabyte (MB) maximum mailbox size

9.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

9.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

10. ENHANCED MOBILE SATELLITE SERVICES

Enhanced Mobile Satellite Services (EMSS) provides deployed warfighters and partnering agencies with global communications through security and user prioritization enhancements to commercial Mobile Satellite Services (MSS). EMSS includes global handheld voice, data, paging, and sim-less short burst data (SBD) communications and supports up to and including secure security classification.

EMSS is a capability provided by DoD that features global data transfer and securable voice communications. The service allows real-time access to other EMSS users, the SBU Voice and commercial U.S. and international telephone networks through the Iridium satellite network.

The EMSS handsets enable the warfighter to communicate with the SBU Voice, Public Switched Telephone Network (PSTN), and SBU IP Data services by leveraging the EMSS gateway that interfaces with those services. If those services were unavailable, EMSS mission partners would be able to communicate only with other EMSS mission partners with EMSS handsets.

10.1 Features

- Secure voice – Encrypts voice communications using National Security Agency (NSA) Type-1 devices

- Prioritization – Mission Partners can allow or deny access to the service in the event of a national emergency
- Basic Telephony – Mission Partners can place or receive a secure call
- Circuit-Switched Data – Provides Mission Partners with a means of communicating (e.g., transmitting and receiving) high-capacity data with data terminal equipment
- Sim-less SBD Service – Provides a non-circuit-switched high-capacity means of transmitting and receiving packets of data to and from compatible SBD subscriber devices
- Paging Services – Mission Partners can receive numeric or text pages
- Router Unrestricted Digital Information Connectivity Solution (RUDICS)/Apollo – Custom devices in the field may connect to servers on the SBU IP Data and provides no additional service logic beyond a transport pipe by which to transmit partner data

10.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

10.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for EMSS.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

11. ENTERPRISE SHAREPOINT SERVICE

Enterprise SharePoint Service (ESPS), a cloud service in the Pipeline, is a dedicated SharePoint hosting service providing Combatant Commands, Military Services, and DoD Agencies a flexible web-based hosting solution which includes a robust set of tools and services to help users manage information and collaborate effectively. Based on the Microsoft SharePoint 2010 platform, this service will provide users with the ability to create and manage mission, community, organization, and user-focused sites for collaboration. Users will be able to manage site collections and content, and distribute allocated storage among their site collections without the additional burden of managing the infrastructure. DISA will manage the multi-tenant environment and provide full lifecycle service for applications, computing, storage, and network infrastructure.

This service offering uses a per-user pricing model, and can be a shared service or dedicated hosting, based upon your needs.

11.1 Features

11.1.1 Standard Features

- Global access across the world
- 99.9% Availability
- Level II Service Desk support
- CAC enabled authentication
- Content and Records Management in a SharePoint environment
- Online discussion areas, shared document and meeting workspaces, document libraries with version control, and surveys
- Out-of-the-box content management features for documents, records, and web content
- Ability to search SharePoint site content across your block of service or within sub-sites
- Non-Secure Internet Protocol Routing Network (NIPRNet)/Secure Internet Protocol Routing Network (SIPRNet) accessible to private and public content publishing
- Dedicated servers, networks, and physical space in DECCs

11.1.2 Optional Features

- Additional storage to accommodate growth
- Enhanced Enterprise SharePoint administration tools
- Site-to-site COOP/Disaster Recovery capability

11.2 Rates

Not yet available.

11.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

12. FORGE.MIL

Forge.mil, a cloud service, is a family of services provided to support the DoD's technology development community. The system currently enables the collaborative development and use of open source and DoD community source software. These initial software development capabilities are growing to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. It is available as a community service, or as a private service on both the unclassified and classified networks.

12.1 Features

Forge.mil is a DISA-led activity designed to improve the ability of the DoD to rapidly deliver dependable software, services and systems in support of net-centric operations and warfare. Forge.mil will:

- Enable cross-program sharing of software, system components, and services
- Promote early and continuous collaboration among all stakeholders (i.e., developers, material providers, testers, operators, and users) throughout the development life-cycle
- Rapidly deliver effective and efficient development and test capabilities for DoD technology development efforts
- Help protect the operational environment from potentially harmful systems and services
- Encourage modularity so that large programs to be developed, fielded, and operated as a set of independent components can evolve and mature at their own rates
- Eliminate duplicative testing and improve dependability by adopting common test and evaluation criteria supported by standard testing tools and methods

12.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

12.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

13. GLOBAL CONTENT DELIVERY SERVICE

Global Content Delivery Service (GCDS), a cloud service, provides a DISN enterprise level service to accelerate delivery and improve reliability of web applications. GCDS is a globally distributed computing platform comprised of a mesh network of content delivery nodes deployed across the DISN, including both SBU IP and Secret IP Data networks. GCDS leverages commercial Internet best practices to provide state-of-the-art web content and web application delivery via standard web protocols, HTTP and HTTPS.

GCDS is fully accredited with Authority to Operate (ATO) and continues to expand its reach and capabilities to soon include network repository, global load balancing, video/audio streaming, and Java 2 Enterprise Edition (J2EE) support.

An additional service of the GCDS program management office (PMO) is the System Network Availability Performance Service (SyNAPS). Our partners purchasing GCDS are provided with performance metrics from SyNAPS and can access their sites' performance data/reports via a partner portal; two SyNAPS transactions per digital domain uniform resource locator (URL) are available at no additional charge. An example of the two free transactions can include a performance/availability metric on a screen or keystroke pattern. The report can show the transaction's metrics for our partner's origin site and GCDS (two transactions). If our partners want additional transactions, those can be purchased separately.

13.1 Features

13.1.1 Standard Features

DISA will plan the deployment logistics, expected service levels, and other program specific criteria. The managed service provider will provide the servers to DISA for GCDS as well as all related software and assist with network design and installation of the servers.

The roles and responsibilities of the managed service provider include the following:

- Monitoring and management of the infrastructure networks and equipment
- Professional services, integration services, and partner care (including help desk)
- Local system administration and remote group administration of the GCDS global network performed by the GCDS managed service provider.
- Two SyNAPS transactions per digital domain URL

GCDS will deliver content that is developed and maintained by the application/content owner. The transmission must process through port 80 (HTTP) or port 443 (HTTPS). GCDS is not a hosting environment but an expansion of the web applications infrastructure. GCDS minimizes or eliminates the requirement to forward deploy additional servers and personnel to reach the targeted audience. The application/content owners will assume all responsibilities associated with the development, initial installation, testing, and contingency operations decisions for the content, and are ultimately responsible for the security of the platforms they manage.

13.1.2 Optional Features

- GCDS NetStorage

One of the main goals of DoD organizations providing mission critical content on SBU IP and Secret IP Data networks is to offer the best end-user experience possible to aid the warfighter. This can be achieved by quickly and reliably delivering rich media files. However, storing and maintaining a large collection of on-demand files, including electronic images, geo-spatial imagery, streaming media files, software, documents, and other digital objects is both technically challenging and resource intensive. It requires a significant investment in racks of redundant servers as well as constant upkeep, including the management of administrative details.

GCDS NetStorage is not local storage normally housed in a DISA DECC, but is storage within the Cloud available to all GCDS nodes worldwide.

GCDS NetStorage is a secure, DoD enterprise solution that eases the burdens associated with data storage. NetStorage consists of multiple terabytes of storage capacity, geographical distribution/replication, a massively scalable architecture, and proprietary mapping and routing technology. By using this fault-tolerant storage service, partners can make their rich media content available to users on demand, anytime and anywhere.

13.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

13.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

14. IBM MAINFRAME APPLICATION HOSTING

DISA will host DoD IBM applications using DISA-provided hardware, operating systems and labor. DISA will provide all hardware, operating system software, infrastructure and systems administration for partner-owned applications.

14.1 Features

14.1.1 Standard Features

The following services are included in the rates:

- System Administration
- Security
- Data Communications
- ESM Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- MIAP
- Capacity Planning

14.1.2 Optional Features

Available upon partner request and will be charged directly to the partner in addition to any costs associated with rate-based services. Optional services include:

- Application Support
- Dedicated Logical Partition (LPAR)
- Dedicated IBM Mainframe
- COOP/Service Continuity

14.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

14.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

15. IBM MAINFRAME Z/LINUX APPLICATION HOSTING

z/Linux runs the Linux operating system (OS) on special mainframe hardware. This mainframe hardware, called an Integrated Facility for Linux (IFL) engine, is specifically designed by IBM to run Linux workloads.

DISA's z/Linux platform offers many of the benefits of the traditional mainframe environment combined with the strength of Linux. These benefits include:

- Mainframe hardware reliability and redundancy
- Quick scalability with minimal disruption
- Strong disaster recovery solution
- Rock solid performance

Our partners pay based on Central Processing Unit (CPU) usage, so this is a true pay-for-what-you-use model. Additionally, our partners may be able to reduce their software license costs by having many z/Linux OEs on very few mainframe engines. So, if several OEs use the same software (i.e., the Oracle Database Management System), all our partners who use that software (Oracle, in this case) can share the cost. This eliminates the need for each of our partners to pay for discrete licenses and maintenance.

DISA will host DoD IBM z/Linux applications using DISA-provided hardware, operating systems and labor.

15.1 Features

15.1.1 Standard Features

The following services are included in the rates:

- System Administration
- Security
- Data Communications
- ESM Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- MIAP
- Capacity Planning

15.1.2 Optional Features

Because different partners require different levels of support, DISA provides choices from the following supplemental services. Each service has its own set of rates, priced per OE on the z/Linux platform. However, if a partner has a uniquely large workload, DISA will work with the partner to develop an agreeable labor support cost method outside of these rates.

- Database Administration
- 24 x 7 System Administration
- 24 x 7 Database Administration
- 24 x 7 Application Support
- Local Operational Recovery

15.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

15.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

16. INFORMATION ASSURANCE STANDARDS AND TRAINING

IA standards and training developed for and used throughout DoD to secure computing devices and increase cyber defense awareness.

16.1 Features

IA Standards and Training features FSO provides in support of secure computing for the war-fighter's networks and systems.

- STIG/Checklist Development – Develop STIG or Checklist to support a specific technology or situation. This will be sufficient to provide configuration settings and parameters for the assured operation within the DOD environment.
- STIG/Checklist Maintenance – Maintain STIG and Checklist to respond to technology changes.
- Develop Training – Develop IA training for a specific system or function.
- Maintain Training – Maintain IA training for a specific system or function based on technology and procedural changes.

- Training Management Support – Conduct training needs assessments, schedule classes, provide logistics for the conduct of the classes, and collect and evaluate feedback.
- Conduct Training – Conduct on-site IA classroom training.
- IA Support Environment (IASE) Support – Manage the IASE. This includes content management and at times collaboration facilitation.
- IA/IT Policy Review – Review IA and IT policy and directives for feasibility and applicability to the DISA IA mission support area.

16.2 Rates

In Fiscal Year 2013, FSO is proposed to become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule.

Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

16.3 Additional Information

Additional service and ordering information can be found by emailing or calling FSO.

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO E-Mail	FSO_SLM@disa.mil

17. INTERNATIONAL MARITIME SATELLITE

The International Maritime Satellite (INMARSAT) services utilize a number of different satellite services to provide warfighters with worldwide access and GIG connectivity for diversity, redundancy and availability. The INMARSAT service provides full range of mobile telecommunications airtime services, equipment and maintenance. The service provides warfighters with access to SBU IP Data, Secret IP Network Data, TS/SCI IP Data, SBU Voice and Multilevel Secure Voice to meet their voice and data requirements and supports up to and including TS/SCI security classification.

17.1 Features

17.1.1 Standard Features

- Traditional Voice calls, low-level data tracking systems, high-speed internet and data services, distress and safety services
- Mobile Integrated Services Digital Network (ISDN) services used for videophone
- Always-on capability where the users are only charged for the amount of data they send and receive (applicable to Broadband Global Access Network (BGAN) and Mobile Packet Data Service)

17.1.2 Optional Features

- BGAN service – simultaneous voice and broadband data communications across most of the world's landmass
- Fleet Broadband – maritime broadband voice and data communications
- Swift Broadband – aeronautical broadband voice and data communications

17.2 Rates

For assistance in obtaining INMARSAT pricing, potential partners should refer to the COMSATCOM Services Branch (CSB) website at:
<http://www.disa.mil/satcom/ss1.html>.

17.3 Additional Information

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for INMARSAT.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

18. MULTILEVEL SECURE VOICE

The Multilevel Secure Voice service provides DoD with high-quality secure voice telephone and conferencing services for end-to-end use by DoD-authorized users. Provision of this service is in accordance with national security directives in support of Command and Control (C2) and crisis management mission functions. This service supports up to and including Top Secret (TS) security classification.

The Multilevel Secure Voice service includes a range of assured services to C2 users and their missions in an environment of a robust and feature-rich set of capabilities. This service is provided at major C2 facilities (i.e., the National Military Command Center (NMCC) and COCOM headquarters) interconnected through a cryptographically secured network. The service is the core of a DoD Global Secure Voice System (GSVS) during peacetime, crisis and time of conventional war by hosting national-level conferencing and connectivity requirements and providing interoperability with both DoD tactical and strategic communities.

18.1 Features

- High-quality, secure telecommunications for C2 and crisis management
- Extensive, secure voice conferencing capabilities with conference management
- DIA-accredited multilevel security (MLS) capability
- Interoperable service with other networks such as commercial, Voice over Internet Protocol (VoIP), Defense Switched Network (DSN), Voice over Secure Internet Protocol (VoSIP), Joint Worldwide Intelligence Communications System (JWICS), satellite, etc
- User-dialed secure connections and conferencing to senior DoD civilian and allied decision makers within the secure voice service Communities of Interest (COI) as well as:
 - Flash Override – considered a capability, not a level of precedence. Exercising this capability preempts calls of all other levels or precedence

- Flash – preempt immediate, priority, and routine calls
- Immediate – preempt priority and routine calls and are reserved for communications pertaining to situations that gravely affect the security of national and allied forces
- Priority – preempt routine calls and are reserved for communications requiring expeditious action by called parties furnishing essential information for conducting government operations
- Routine – routine precedence applies to official government communications that require rapid transmission by telephonic means, but do not require preferential handling. A routine call does not preempt any other call

18.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

18.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

CJCSI 6215.02C governs the approval authority required for the Multilevel Secure Voice precedence type of service.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for Multilevel Secure Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

19. NETWORK DEFENSE

FSO provides Network Defense capabilities including features needed to ensure warfighter success through secure networks.

19.1 Features

Network Defense features support securing of warfighter networks.

- Network Security Monitoring & Incident Reporting & Attack, Sensing, and Warning (AS&W) – Service provided to CNDSP subscribers which utilizes an incident reporting system for complete and meaningful incident report recording and rapid distribution to DoD channels and law enforcement/intelligence communities.
- Incident Response and Recovery Team (IRRT) – Deployable emergency response team designed to assist sites in locating and recovering from network intrusions.
- System Architecture, Analysis and Testing (SAAT) – Test the security and stability of the associated program using a variety of techniques.
- Malware Analysis – Reverse engineering of malware to determine the functionality of the software and to identify artifacts that can be utilized to locate additional infections.
- Media Analysis – Analysis performed on system media to identify attack vectors, tools used, exploited software, and increase detection ability on networks and hosts.
- Trends Analysis – Detailed analysis of IA/CND data from varying sources, to include compliance and intrusion data to identify and analyze trends, creating value-added products and reports for the enhancement of IA/CND policies, technologies, tactics, and training products.
- CNDSP Exercise Support – Provides critical IA-based exercise support in various theater and global exercises.
- Red Teaming – The Red Team is a focused, threat-based operation by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to develop recommendations for the improvement of the security posture and operational CND capabilities and procedures utilized to protect networks and systems.
- Penetration Testing – Involves approaches to vulnerability identification, enumeration, and attempted exploitation to determine the value and effectiveness of a network, system, or application's security configuration. Penetration testing is coordinated and conducted primarily in the open in accordance with a signed authorization by the system owner.

- Vulnerability Assessment, Analysis & Trending – Vulnerability Assessment, Analysis, and Trending is conducted at the request of network owners in support of, or in augmentation to, the partner’s internal, DoD mandated vulnerability scanning and assessment actions.
- Non-materials Solutions Development – The rapid development of tactical capabilities in response to an emerging threat.
- IA Training Program Support – Provides hands-on technical assessment training for networks, operating systems and applications.
- CNDSP Subscriber Services Support – Options for all or partial CNDSP Tier 2 services (Protect, Detect, Respond and Sustain)
- Sensor Implementation – The fielding and implementation of CND technologies into the operational environment in support of Tier 2 and 3 CNDSP.
- Sensor Configuration Management – Configuration and baseline support for managed sensors.
- Sensor CONOPs/TTP Development – Development of CONOPs for sensor solutions and supporting TTPs.
- Sensor Trouble Desk Escalation – Trouble shooting assistance for sensor issues that surface from the sensor grid.

19.2 Rates

In Fiscal Year 2013, FSO is proposed to become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule.

Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

19.3 Additional Information

Additional service and ordering information can be found by emailing or calling FSO.

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO E-Mail	FSO_SLM@disa.mil

20. ORGANIZATIONAL MESSAGING SERVICE

The Organizational Messaging Service provides a range of assured services to our partner communities that include the military services, DoD agencies, COCOMs, non-DoD U.S. government activities, and the Intelligence Community (IC). These services include the ability to exchange official information between military organizations and to support interoperability with Allied nations, non-DoD activities and the IC operating in both the strategic/fixed-base and the tactical/deployed environments. This service supports up to and including Top Secret Collateral (TS/C) security classification.

20.1 Features

- **Guaranteed Message Delivery** – all recipients of a message receive the message or the service returns a non-delivery notification to the message originator giving the reason for each unsuccessful delivery attempt.
- **Priority Transmission** – Defense Messaging Service (DMS) servers allow users to specify the precedence of each message they originate subject to controls that limit the precedence levels at which each user is authorized to originate a message.
- **Message Confidentiality, Integrity, and Non-Repudiation** – DMS guarantees this feature through NSA-approved message cryptography and link encryption with audit mechanisms that support non-repudiation.
- **Security Access Control** – DMS applies these protections to messages based on the message security label and the authorizations assigned to organizations and specific users within those organizations.
- **Interoperability** – This feature is supported between DoD organizations, non-DoD organization, and allied nations.
- **Automated Message Handling** -Operated by the user community and implement message dissemination, storage, search, and retrieval.

- High Service Availability – The system provides a high level of service availability based on equipment, communication redundancy path, COOP sites and alternate routing designs.
- High Security Assurance – The system provides a high degree of security assurance based on strict compliance with security policies and directives, as well as, on the use of the NSA-approved and supported cryptographic suite.

20.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

20.3 Additional Information

Partners order DMS service from Service or Agency operated Area Control Centers (ACCs). The Services/Agency ACCs establish connectivity to the DMS infrastructure in accordance with DMS Interim Procedure 09-V15 (Procedures and Guidelines for Establishing DMS Organizational Users dated 28 March 2008).

The DGSC serves as the mission partner POC for Organizational Messaging.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

21. RAPID ACCESS COMPUTING ENVIRONMENT

The Rapid Access Computing Environment (RACE), a cloud service, provides a streamlined process for the provisioning and subsequent development; testing; and through the utilization of Enterprise Mission Assurance Support Service (eMASS) and VMS, streamlined certification, accreditation and deployment of applications to a DISA DECC. DISA packages hosting, networking, security and connectivity together as a service to DoD partners. RACE is available to all our DoD partners, including all Services and Agencies, as well as their corporate design partners. Users can acquire server capacity rapidly, for short or long-term use, using Operations and Maintenance (O&M) or Research, Development, Test & Evaluation (RDT&E) funding, without the need for capital acquisitions.

21.1 Features

This is a service allowing authorized partners to procure and provision virtual servers using a self-service web portal, have the test and development servers available for use by the next business day, and have the follow-on comparable production servers available within seven to 10 days.

21.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

21.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

22. SECRET INTERNET PROTOCOL DATA

The Secret IP Data service provides point-to-point connectivity to mission partners. It also provides access to data, e-mail, and web services content up to and including Secret security classification.

The Secret IP Data provides IP-based secret information transfer across DoD for official DoD business applications such as e-mail, web services, and file transfer. The Secret IP Data service gateway function provides DoD mission partners with centralized and protected connectivity to federal, IC, and allied information at the secret level. The Secret IP Data service includes IP-based secret information exchange within DoD (DoD intranet) and centralized, gateway external network information exchange (i.e., the extranet). The intranet function provides access to a joint, shared DoD environment at the Secret security classification for the exchange of information among DoD components.

22.1 Features

- Connectivity
 - Classification Segmentation—Joint, DoD-wide enterprise internetworking enables the exchange of secret information.
 - Rate-Limited Access Bandwidth—IP data rate limited to the partner-requested access bandwidth up to the maximum supported by the interface.
 - Control and Routing Exchange—Static configuration or dynamic updates using the Border Gateway Protocol (BGP) that are supported for IP routing between the DISN edge and Customer Edge (CE) routers.
 - Dial-Up Access—Remote workstation access to the Secret IP Data service through the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN) and Secure Telephone Unit or Secure Terminal Equipment (STE).
- IA Protection
 - Access Load-Sharing and Diversity—This feature supports multiple access links to improve service survivability. Options for ordering access circuits include load-sharing (active/active) and primary with secondary backup (active/standby) for interface, node, or site diversity to meet site C2 survivability requirements.
 - External Network Gateways for Perimeter Protection—This feature provides protected, centralized interfaces to external networks. The classified federal DMZ and releasable DMZ provide secure connectivity to the IC and other federal government and allied networks operating at the secret level.
- Network Management Features
 - Configurable Aggregate Access Bandwidth—The service access bandwidth will be configurable up to the maximum supported by the access physical interface through the service portal.
 - Configurable Service Class Access Bandwidth—The allocation of the access interface aggregate bandwidth among service classes will be configurable through the service portal. Ingress traffic policing will enforce the allocation within each service class, and egress traffic policing (inelastic/real-time) or shaping (preferred elastic and elastic classes) will manage bandwidth within each service class based on information priority. Default service will be best effort (100 percent allocation to the elastic service class) for Mission Partners that do not require Class of Service (CoS)-enabled service assurance.

22.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

22.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for Secret IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

23. SECRET TEST AND EVALUATION INTERNET PROTOCOL DATA

The Secret Test and Evaluation (T&E) IP Data service provides a “test and train like we fight” joint operational environment to support a variety of T&E COI. These COIs have the capability to conduct development, certification and operational T&E activities in an operationally relevant T&E environment. This service supports up to and including Secret security classification.

23.1 Features

23.1.1 Standard Features

- Plain-text information exchange at the secret classification level.

- DISA-managed High Assurance Internet Protocol Encryption (HAIPE™) of the partner data for transport across the DISN T&E network.
- IP routing on the CE that is configured by the user and IP packets that are routed by the T&E network transport based on static routes managed by DISA CONUS, which are configured to provide full-mesh connectivity established among all T&E HAIPE™ devices.
- Support for partner-established VPN/tunnel connection from CE to CE using Generic Routing Encapsulation (GRE) or IP Security tunnels.

23.1.2 Optional Features

- Provisioning of CE connection for Secret T&E IP Data Meet-Me (conferencing) service.
- Site support not to exceed 1,000 man-hours that include end-to-end coordination of implementation service, event support, user/premise equipment installation, circuit provisioning and engineering maintenance, troubleshooting, incidental materials, and related travel.

23.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

23.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for Secret T&E IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

24. SECURE FILE GATEWAY RELAY SERVICE

The Secure File Gateway (SFG) Relay Service is a technical solution for ensuring secure data transference between DoD sites and between commercial sites interfacing with the DoD. The resulting solution attempts to address impending DoD security policy changes, the increasing administration workloads as associated with other file transfer services, and the functionality requested by our many partners.

24.1 Features

- Security
- Administrative Savings
- Partners can configure, update, and manage their own file transfer process or processes
- E-mail notifications for file receipt, relay success, and relay error results
- Enables simplified scripting capabilities via the partner's relay configuration file
- Provides tools for data encryption, data transformation, and additional security checks
- Entrusts each partner with aggregated relay logs, containing status, resource and security details
- Guarantees data delivery, enables Secure File Transport Protocol (SFTP) checkpoint restarts and provides for data transfer self-healing
- Obtains resolutions from our partners for common errors (e.g. Login failed, Network unreachable, et al)

24.2 Rates

Where applicable, to find the Department of Defense (DoD)-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

24.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the Service Level Agreement (SLA) which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling the Computing Services Directorate (CSD).

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

25. SECURE MOBILE ENVIRONMENT PORTABLE ELECTRONIC DEVICE

The Secure Mobile Environment-Portable Electronic Device (SME-PED) service provides DoD personnel with wireless mobile communications leveraging continuing investments in intelligence, reconnaissance and C2 capabilities. The service provides personal communication devices with integrated wireless e-mail, Web browsing and document viewing has enabled a new breed of mobile workforce and supports up to and including TS security classification.

25.1 Features

- Mobile access to classified systems using the SBU IP Data and Secret IP Data services
- Type 1 and non-type 1 encryption for data and voice
- Connection to DoD voice gateway for Multilevel Secure Voice service access
- Connection to the Multiple Commercial Wireless Service (MCEP) for SBU and Secret IP Data services access
- Single entry point for enclaves requiring multiple diverse wireless network services
- Managed end-to-end service with common reliability and security characteristics

25.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

25.3 Additional Information

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

The DGSC serves as the mission partner POC for SME-PED.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

26. SENSITIVE BUT UNCLASSIFIED INTERNET PROTOCOL DATA

SBU IP Data provides point-to-point connectivity to DISA mission partners. This unclassified IP data service for Internet connectivity and information transfer supports DoD applications such as e-mail, web services, and file transfer. The SBU IP Data service also provides DoD mission partners with centralized and protected access to the public Internet. This service supports up to and including SBU security classification.

26.1 Features

- Connectivity
 - Rate-Limited Access Bandwidth — IP data rate limited to the partner-requested access bandwidth up to the maximum supported by the interface.
 - Control and Routing Exchange — Static configuration or dynamic updates using the BGP that is supported for IP routing between the DISN Edge and CE routers.
- IA Protection
 - Access Load-Sharing and Diversity — Supports multiple access links to improve service survivability. Options for ordering access circuits include load-sharing

- (active/active) and active primary with secondary backup for interface, node, or site diversity to meet site C2 survivability requirements.
- External Network Gateways for Perimeter Protection — Provides protected, centralized interfaces to external networks. The internet access points, or gateways, screen DoD network assets from Internet threats and provide secure connectivity to the IC and other federal government and allied networks operating at the unclassified level.
- Network Management
 - Network Time—Network time protocol distributes the time-of-day clock to partner CE routers for system time synchronization and event correlation.

26.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

26.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for SBU IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

27. SENSITIVE BUT UNCLASSIFIED VOICE

SBU Voice provides a global inter-base, non-secure, or secure, DoD telecommunications service for C2 use by DoD-authorized users in accordance with national security directives. SBU Voice also provides IP and circuit-switched voice-band data transfer and dial-up videoconferencing. SBU Voice is required to provide assured voice communications to C2 mission partners. Services are provided through the implementation of military unique features, including Assured Service like Multiple Level Precedence and Preemption (MLPP), to support the military C2 functions. This service supports up to and including SBU security classification.

27.1 Features

- Automated Access – SBU Voice services also provide automated access capabilities to the following networks:
 - International gateways to the defense networks of our allies for cost avoidance of international commercial calling (Australia, Canada, North Atlantic Treaty Organization (NATO), New Zealand, and United Kingdom)
 - EMSS
 - Government Emergency Telephone System (GETS)
- Survivable Service – The following features contribute to the survivability of the SBU Voice:
 - No single point of vulnerability will exist for the entire network
 - Transport supporting major installations (base, post, camp, and station, leased or commercial sites/locations) will use physically diverse DISN routes (where possible)
- Assured Connectivity – Special C2 users under the current SBU Voice MLPP scheme (Flash and Flash Override) are provided non-blocking service.
- Interoperable Service – SBU Voice is designed with the capability to permit interconnection and interoperation with similar tactical, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable and IA-accredited as specified.

27.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

27.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

NOTE: There are services that require a connection approval. Information regarding connection approvals can be found at <http://www.disa.mil/connect>.

The DGSC serves as the mission partner POC for SBU Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

28. SERVER APPLICATION HOSTING

The unit of measure for Basic Services is the OE, which DISA defines as an instance of an OS. One physical server could have one copy of the OS installed, in which case the OE is the server itself. However, one physical server could be carved into many partitions (similar to a mainframe), each of which has one copy of the OS installed. (These are called virtual OEs or virtual machines.) Note that we charge Server rates at the OE level, not at the physical server level.

The OS (Windows or Unix) and the number of sockets populated with CPUs will determine the size of the OE (Level 2 to 6). The rates differ based on size and OS.

DISA will host DoD server applications using DISA-provided hardware, operating systems and labor.

28.1 Features

28.1.1 Standard Features

The following services are included in the rates:

- System Administration
- Security
- Level 2 Service Desk Support
- Maintenance costs for the monitoring software the Service Desk uses and costs associated with the DISA communications infrastructure.

28.1.2 Optional Features

Because each partner's processing requirements may differ from the next partner, DISA offers all partners a selection of supplemental services. Each service has its own set of rates, based on the size and type of OS. The rates are per OE. Optional services include:

- Hardware Services
- Application Support
- Web Administration
- Database Administration
- Oracle Database Software Maintenance
- 24 x 7 System Administration
- 24 x 7 Database Administration
- 24 x 7 Application Support
- Cost-Reimbursable (Non-Rate) Services
- COOP/Service Continuity

28.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

28.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

29. Storage Support for Server-Based Applications

Our partners purchasing Server services are offered a wide array of storage opportunities that allow DISA to provide the level of service required to meet maximum acceptable data loss.

Rate-based server storage pricing is based on the GB (raw) storage allocated per month and the level of service requested by the partner for data recovery, not application restoration based on RTO and RPO. Additional levels are cumulative, for example, R1 is (L1+R1) * GB storage.

The table below shows the options available for operational or local recovery. The first entry is included as part of the L1 storage rate and is based on the use of locally available backup media, to recover on existing production storage capacity. Entries L2 and L3 are advanced local data recovery options. Please note that local recovery will not satisfy the COOP/Service Continuity requirements detailed in DoDI 8500.2, which mandates a remote recovery strategy at a predetermined location.

Level	Description	Maximum Data Loss
L1	Default Local	7 Days
L2	Operational Local	24 Hours
L3	High-Availability Local	8 Hours

29.1 Features

29.1.1 Standard Features

- Default Local/Operational Recovery (L1)

Level	Description	Maximum Data Loss
L1	Basic/Default Local	24 Hours to 1 Week
Hardware	Depreciation and Maintenance	
	Infrastructure – switches, backup media	
	Racks, cables	
Software	Standard OE (SOE) and other storage resources	
Labor	Storage Administration	
	Service Desk Support	
Backup Services	Standard weekly Operational Backup (one [1] copy onsite, retained four [4] weeks) designed for local recovery only.	
	Incremental daily Operational Backups (retained two [2] weeks onsite) designed for local recovery only.	
	Standard weekly COOP Backup (one [1] copy offsite, retained four [4] weeks) designed for remote recovery.	
Data Center Services	Security	
	Facilities	
	Networks	
	Tech Refresh (Storage Array)	
	Service Desk	

29.1.2 Optional Features

Local/Operation Recovery, or “recovery in place,” is a program designed to provide continuity in the event of an outage affecting the equipment, software and/or data that make up the application infrastructure but that leaves the primary facility operating and accessible. Based on the solutions selected, there are three advanced options for operational recovery.

- Operational Local/Operational Recovery Combination 1 (L2)
- High-Availability Local/Operational Recovery Combination 2 (L3)
- Cost Reimbursable Services

Options	Description	Maximum Data Loss
Local/Operational Recovery	Recovery in place using production equipment and backup data	7 Days
Advanced Local/Operational Recovery Combination 1	Recovery in place using production equipment and backup data in a near-online state	24 Hours
Advanced Local/Operational Recovery Combination 2	Recovery in place using production equipment and frequently updated backup data in a near-online state and/or designated remote site	8 Hours

NOTE: DoDI 8500.2 requires recovery strategies to include a designated site for remote recovery efforts. Operational recovery options will not, by themselves, satisfy the stated requirements for continuity.

29.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

29.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

30. SYSTEM NETWORK AVAILABILITY PERFORMANCE SYSTEM

SyNAPS, utilizing Hewlett-Packard (HP) Business Availability Center (BAC) Infrastructure (formerly Mercury Topaz), will provide transaction performance monitoring. SyNAPS utilizes synthetic users to monitor both user and system initiated web traffic between client machines and servers throughout the world. SyNAPS will provide early warnings of availability and performance problems, help prioritize and accelerate problem resolution based on business impact, and ensure compliance with SLAs.

30.1 Features

From a single management console, with the SyNAPS Probe component, SyNAPS will be able to potentially manage thousands of users' behavior and access points across multiple web-based applications. SyNAPS functionality will allow for user performance delivery monitoring in real-time and the utilization of enterprise applications to the warfighter.

Another component of SyNAPS is the SyNAPS Client Monitor. As a SyNAPS data collector, the SyNAPS Client Monitor will proactively monitor enterprise applications in real-time, identifying application performance problems before users are aware a problem exists. The SyNAPS Client Monitor will enable the application owner to monitor sites from various locations and will be able to emulate the end-user's experience. This will allow the application owner to assess site performance from different client perspectives.

SyNAPS partners will experience the SyNAPS dashboard for personalized results. The dashboard is a role-based, user-emulated, and customizable graphic user interface (GUI) that will provide a common environment combining real-time application stability and historical performance data for immediate review. SyNAPS partners will be able to create personalized reports from dozens of predefined templates, enabling the application owner to focus on the key performance indicators (KPIs).

30.2 Rates

Where applicable, to find the Department of Defense (DoD)-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

30.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the Service Level Agreement (SLA) which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling the Computing Services Directorate (CSD).

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

31. TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION INTERNET PROTOCOL DATA

The TS/SCI IP Data service is a secure high-speed multimedia communication service between Sensitive Compartmented Information (SCI) users designed to support the DoD Intelligence Information System (DoDIIS) community through the Defense Intelligence Agency (DIA) Regional Support Centers (RSCs). This service supports up to and including TS/SCI security classification.

31.1 Features

- Quality of Service (QoS) for guaranteed performance of multiple application types
- Multifaceted network management and control capability
- Extends to non-fixed and SATCOM-based sites for tactical users
- Supports voice and video

31.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

31.3 Additional Information

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

The DGSC serves as the mission partner POC for TS/SCI IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

32. TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION VIDEOCONFERENCING

The TS/SCI Videoconferencing service provides secure video communication between SCI users and is designed to support the room-based studio quality and desktop conferencing to the DoDIIS community through the DIA RSCs. The service provides global VoIP communications for DoD mission partners within SCI enclaves connected to the TS/SCI IP Data service, and uses stream-based encryption for private video traffic. This service supports security classifications up to, and including, TS/SCI.

32.1 Features

- Room-based video teleconferencing (VTC) features include the following:
 - High-quality, studio-based videoconferencing
 - Software scheduling assistant
 - Integrated multimedia display capability
- Desktop VTC features include the following:
 - Ad hoc videoconferencing
 - Integrated directory service

32.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

32.3 Additional Information

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

The DGSC serves as the mission partner POC for TS/SCI Videoconferencing.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

33. TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION VOICE

The TS/SCI Voice service provides secure communication between SCI users up to and including TS/SCI security classification. It is designed to support the DoDIIS community through the DIA RSCs. The service provides global Voice over Internet Protocol (VoIP) communications for DoD within SCI enclaves connected to the TS/SCI IP Data service, and uses stream-based encryption for private voice traffic.

33.1 Features

- Intelligence Community-wide calling through gateway connectivity to the National Secure Telephone System (NSTS)
- QoS for guaranteed performance of multiple application types
- Multifaceted network management and control capability
- Extends to non-fixed and SATCOM-based sites for tactical users
- Supports data and video

33.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

33.3 Additional Information

Our mission partners order DISN telecommunication services via the DDOE application located at <https://www.disadirect.disa.mil>.

The DGSC serves as the mission partner POC for TS/SCI Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

34. UNISYS MAINFRAME APPLICATION HOSTING

DISA will host DoD Unisys applications using DISA-provided hardware, operating systems and labor. DISA will provide all hardware, operating system software, infrastructure and systems administration for partner-owned applications.

34.1 Features

34.1.1 Standard Features

The following services are included in the rates:

- System Administration
- Security
- Data Communications
- ESM Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- MIAP
- Capacity Planning

34.1.2 Optional Features

Available upon partner request and will be charged directly to the partner in addition to any costs associated with rate-based services. Optional services include:

- Application Support
- LPAR
- Dedicated Unisys Mainframe
- Classified COOP/Service Continuity

34.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

34.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

35. VOICE AND CIRCUIT SUPPORT

NOTE: This support is available to our local Columbus, OH area partners only

Voice and Circuit Support services are divided into four support categories:

- Voice Services
- Data Communications Support
- Local Area Network (LAN) Support

- Electronic Systems Support

All services listed are available at the request of our local Columbus partner, and the exact terms and conditions are outlined with the description of each service.

35.1 Features

35.1.1 Standard Features

- Voice Services Telephone System Support

35.1.2 Optional Features

- Voice Services
- Data Communications Support
- LAN Support
- Electronic Systems Support

35.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

35.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

36. VOICE OVER SECURE INTERNET PROTOCOL

The VoSIP service provides a cost-effective, reliable, and secure means of classified voice communications, secret only, for C2 and non-C2 mission partners with the capability to communicate directly using point-to-point or conference calling. It does provide a media/voice interface (gateway) to the circuit-switched network providing interoperability between the VoSIP service and the Multilevel Secure Voice service. This service supports up to and including Secret security classification.

VoSIP provides a permanent and long-term solution for global secure communications among all sites that are part of the VoSIP and secure voice services.

- The process for connecting to VoSIP is defined in the VoSIP/Classified Voice and Video over Internet Protocol Connection Guide (<https://www.us.army.mil/suite/doc/23568699>).

36.1 Features

- Voice
 - Provides an interface between the IP Telephony and the circuit-switched network
 - Provides the full range of supplemental user features (e.g., call hold, call transfer, and abbreviated dialing) available from IP telephony
- Security
 - Uses a separate IP address space for voice communications
 - Firewalls are installed at each VoSIP core site and access control lists are deployed on all routers and gateways to ensure that only permitted traffic flows through them
 - Maintains compliance with IA Vulnerability Alert (IAVA) monitoring and implementation according to the guidelines in the IAVA Management Plan
 - The VoSIP services features an identity management solution (IMS) designed to discover, identify and track the use of network resources
- Emergency Access
 - Emergency calling based on local policies of each enclave (e.g., Network Operating Center [NOC], Theater Communications Control Center or any other emergency activation capability)
 - The Cisco Unified Meeting Place supports emergency access with a host of features (e.g., conferencing features, centralized identity management, access control security)

mechanisms, host intrusion and detection, directory services, and interoperability with secure voice services)

36.2 Rates

Service rate information is located under Inventory and Billing on DISA Direct at <https://www.disadirect.disa.mil>.

36.3 Additional Information

The DISN Telecommunications SLA, located on DISA Direct at <https://www.disadirect.disa.mil>, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

The DGSC serves as the mission partner POC for VoSIP.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC e-mail	SBU IP Data e-mail: DGSC@CSD.DISA.MIL Secret IP Data e-mail: DGSC@COLS.CSD.DISA.SMIL.MIL

37. WEB HOSTING

DISA can provide three levels of the web hosting cloud service, ranging from “simple” to “complex.” The standard services are based on the use of Microsoft Windows Standard/Internet Information Services (IIS) or Linux/Apache on DISA-provided hardware. Web Hosting service offerings include Mission Assurance Category (MAC) III remote recovery. The offerings are summarized as follows:

- Bronze – Simple to intermediate-sized web sites, with DISA-supported scripting and small data requirements (less than one GB per site)
- Silver – Intermediate-sized web sites requiring a dedicated operating environment(s) (OE), scripting support, and increased storage requirements (five GB of data per OE)
- Gold – Intermediate-sized to complex web sites requiring a dedicated server, scripting support, and significant storage (20 GB of data)

- NOTE: Restricted WEB authorized web sites (WEB-R) and unrestricted public web sites (WEB-U) are available through the standard rate structure.

37.1 Features

37.1.1 Standard Features

All Web Hosting Levels include the following services:

- Project Management
- Basic services
- Systems Administration (SA)
- Hardware Services
- IA
- Facility Environmentals (Heating, Ventilating, and Air Conditioning [HVAC]; power; Uninterruptible Power Supply [UPS])

37.1.2 Optional Features

Database as a Service (DaaS) is also available, but is currently offered on a very restricted basis, and is only available to those partners that have selected the Bronze or Silver level web hosting service.

Using the DISA Capacity Services approach, the DaaS promotes improved server utilization and reduces operational and environmental impacts created by dedicated servers. DaaS offers partners two OE choices:

- Microsoft Structured Query Language (SQL) Server
- MySQL

37.2 Rates

Where applicable, to find the DoD-approved rates for Cloud Production Systems support, please refer to <http://disa.mil/computing/documents/RatesFY12.pdf>.

37.3 Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information can be found by emailing or calling CSD.

Organization	Contact Information
CSD Phone	CML: 303-224-1660 DSN: 926-1660
CSD E-Mail	CSD_SLM@csd.disa.mil

APPENDIX A – ACRONYMS

The following acronyms are referenced throughout this document.

Acronym	Definition
ACC	Area Control Center
AS&W	Attack, Sensing, and Warning
ATAAPS	Automated Time Attendance and Production System
ATO	Authority to Operate
B2B	Business to Business
BAC	Business Availability Center
BGAN	Broadband Global Area Network
BGP	Border Gateway Protocol
C2	Command and Control
C&A	Certification and Accreditation
CAC	Common Access Card
CCRI	Command Cyber Readiness Inspection
CC/S/A	Combatant Commands, Military Services, and DoD Agencies
CE	Customer Edge
CJCSI	Chairman Joint Chiefs of Staff Instruction
CM	Configuration Management
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COCOM	Combatant Command
COI	Community of Interest
COIN	Community of Interest Network
COMSATCOM	Commercial Satellite Communications
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
CoS	Class of Service
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSD	Computing Services Directorate

CSS	Commercial Satellite Services
DAA	Designated Approving Authority
DaaS	Database as a Service
DDOE	DISA Direct Order Entry
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DGSC	DISN Global Support Center
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIME	Deployment, Implementation, Maturization and Effectiveness
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN-LES	Defense Information Systems Network Leading Edge Service
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	DoD Intelligence Information System
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVS-G	DISN Video Service – Global
DWCF	Defense Working Capital Fund
E-BSC	Enterprise Business Service Catalog
eMASS	Enterprise Mission Assurance Support Service
EMSS	Enhanced Mobile Satellite Services
ESM	Enterprise Systems Management
ESPS	Enterprise SharePoint Service
FSO	Field Security Operations
FTP	File Transport Protocol
FW	Firewall
GAL	Global Address List
GB	Gigabyte

GCDS	Global Content Delivery Service
GETS	Government Emergency Telephone System
GEX	Global Exchange
GIG	Global Information Grid
GISMC	GIG Global Infrastructure Service Management Center
GRE	Generic Routing Encapsulation
GSSC	Global SATCOM Support Center
GSVS	Global Secure Voice System
GUI	Graphic User Interface
HAIPE™	High Assurance IP Encryption
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilating, and Air Conditioning
IA	Information Assurance
IaaS	Infrastructure as a Service
IARR	Information Assurance Readiness Review
IAVA	Information Assurance Vulnerability Alert
IASE	Information Assurance Support Environment
IC	Intelligence Community
IFL	Integrated Facility for Linux
IIS	Internet Information Services
IMS	Identity Management Solution
INMARSAT	International Maritime Satellite
IP	Internet Protocol
IRRT	Incident Response and Recovery Team
ISDN	Integrated Services Digital Network
IT	Information Technology
J2EE	Java 2 Enterprise Edition
JWICS	Joint Worldwide Intelligence Communications System
KPI	Key Performance Indicators
LAN	Local Area Network
LPAR	Logical Partition

MAC	Mission Assurance Category
MB	Megabyte
MCEP	Multiple Commercial Wireless Service
MIAP	Mainframe Internet Access Portal
MLPP	Multi-Level Precedence and Preemption
MLS	Multilevel Security
MQ	Message Queuing
MSP	Managed Service Provider
MSS	Mobile Satellite Service
NATO	North Atlantic Treaty Organization
NetOps	Network Operations
NIPRNet	Non-Secure Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NMCC	National Military Command Center
NOC	Network Operating Center
NS	Network Service
NSA	National Security Agency
NSTS	National Secure Telephone System
OCONUS	Outside the Continental United States
OE	Operating Environment
O&M	Operations and Maintenance
OOB	Out-of-Band
OS	Operating System
OSD	Office of the Secretary of Defense
OWA	Outlook Web Access
PB Collo	Policy-Based Co-Location
PMO	Program Management Office
POC	Point of Contact
PPSM	Ports, Protocols and Services Management
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACE	Rapid Access Computing Environment
RDT&E	Research, Development, Test & Evaluation

RPO	Recovery Point Objective
RRC	Remote Recovery Combination
RSC	Regional Support Center
RSSC	Regional SATCOM Support Center
RTO	Recovery Time Objective
RUDICS	Router Unrestricted Digital Information Connectivity Solution
SA	System Administration
SAAT	System Architecture, Analysis, and Testing
SATCOM	Satellite Communications
SAV	Security Assistance Visit
SBD	Short Burst Data
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SFG	Secure File Gateway
SFTP	Secure File Transport Protocol
SIPRNet	Secure Internet Protocol Routing Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SME-PED	Secure Mobile Environment – Portable Electronic Device
SMTP	Simple Mail Transfer Protocol
SOE	Standard Operating Environment
SSH	Secure Shell
SSL	Secure Socket Layer
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
SyNAPS	System Network Availability Performance Service
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TS	Top Secret
TS/C	Top Secret/Collateral
TS/SCI	Top Secret/Sensitive Compartmented Information
TTP	Techniques, Tactics, and Procedures
UPS	Uninterruptible Power Supply

URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command
VCF	Videoconferencing Facilities
VMS	Vulnerability Management System
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VMS	Vulnerability Management System
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTC	Video Teleconferencing
WAN	Wide Area Network
WEB-R	Restricted WEB Authorized Web Sites
WEB-U	Unrestricted Public Web Sites

APPENDIX B – REFERENCES AND CITATIONS

- CJCS Instruction 6510.01F, February 2011, Information Assurance (IA) and Support to Computer Network Defense (CND)
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
- DoD Directive 5015.2, March 2000, DoD Records Management Program
<http://www.defense.gov/webmasters/policy/dodd50152p.pdf>
- DoD Directive 8500.01E, October 2002, Information Assurance (IA)
<http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>
- DoD Financial Management Regulation 7000.14-R, April 2011
<http://www.defenselink.mil/comptroller/fmr/>
- DoD Financial Management Regulation 7000.14-R, Volume 11B, December 2010, Reimbursable Operations, Policy and Procedures – Working Capital Funds (WCF)
<http://www.defenselink.mil/comptroller/fmr/11b/index.html>
- DoD Instruction 4000.19, August 1995, Interservice and Intragovernmental Support
<http://www.dtic.mil/whs/directives/corres/pdf/400019p.pdf>
- DoD Instruction 5200.01, October 2008, DoD Information Security Program and Protection of Sensitive Compartmented Information
<http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf>
- DoD Instruction 8500.2, February 2003, Information Assurance (IA) Implementation
<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>
- DoD Instruction 8510.01, November 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP)
<http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>
- NIST Special Publication 800-53, August 2009, Recommended Security Controls for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- OMB Circular A-130, February 1996, Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars_a130



Document Source

- All DoD Issuances <http://www.dtic.mil/whs/directives/>
- All OMB Circulars <http://www.whitehouse.gov/omb/circulars/#numerical>