Defense Information Systems Agency

A Combat Support Agency

Defense Information Systems Agency

Computing Services Directorate

Service Catalog

Published Date:

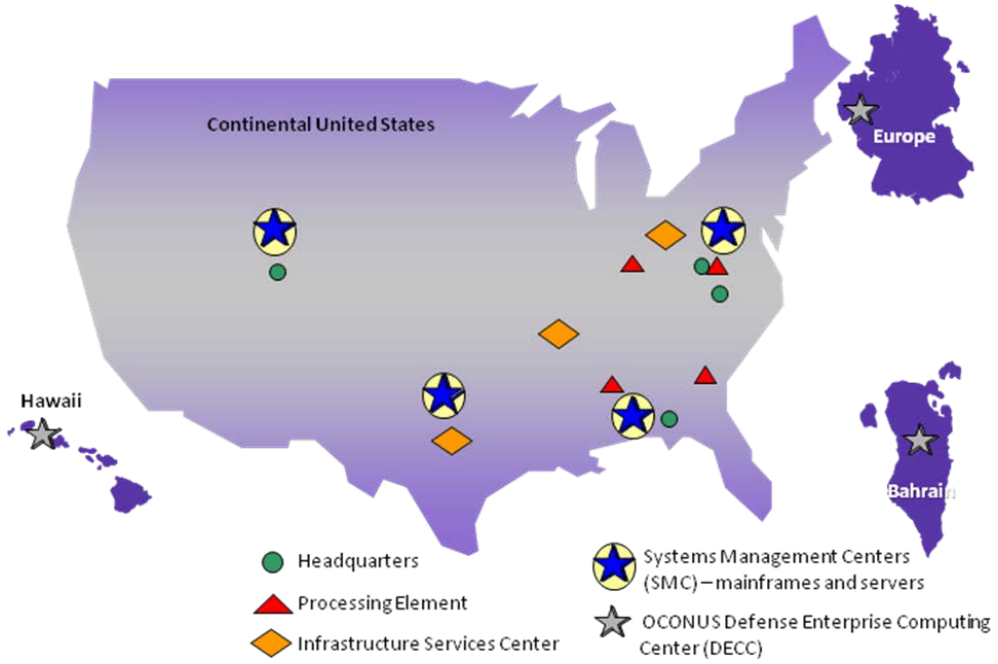
8 August 2011

Version 5.0

Computing Services Hosts, Manages and Supports DoD Enterprise and eBusiness Applications Worldwide

INTRODUCTION

The Defense Information Systems Agency (DISA), Computing Services Directorate (CSD) provides Information Technology (IT) services in response to our Department of Defense (DoD) 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 CSD's mission is to deliver computing information products and services that enable and enhance the ability of our partners to execute their missions.



This Service Catalog describes the services offered by DISA CSD. These include both the primary CSD mission of providing highly efficient and secure raised floor operations for hosting partner systems/applications, and various other services which DISA CSD makes available.

DISA CSD has adopted the Best Practices approach as a framework for operational and business process improvement. Initially, formal plans have been/are being implemented in the following areas:

- *Change Management*
- *Availability Management*
- *Capacity Management*
- *Service Level Management*
- *Incident Management*
- *Problem Management*
- *Configuration Management*

POINTS OF CONTACT

- **DISA CSD Service Level Management (SLM) Division POCs:**

  Comments or suggestions about the Partner Portal or this Service Catalog are welcomed, and should be directed to one of the following:

DISA CSD SLM Hotline	CSD Service Level Manager	CSD Service Catalog Manager
(303) 224-1660 (DSN 926)	(303) 224-1868 (DSN 926)	(303) 224-1732 (DSN 926)
CSD_SLM@csd.disa.mil		

- **DISA CSD Customer Relationship Management Division POCs:**
  - **Chief, Customer Relationship Management Division**

    (301) 225-7209 (DSN 375)
  - **Customer Management Executive (CME) POCs:**

    Questions regarding specific services within this Service Catalog are welcomed, and should be directed to your Service or Agency CME:

Air Force	Army	DFAS/DLA/BTA/US TRANSCOM
(301) 225-7205 (DSN 375)	(301) 225-7214 (DSN 375)	(717) 267-9175 (DSN 430)
DISA	**Joint Staff/COCOM/ OSD/DoD/Classified**	**MHS/TRICARE**
(301) 225-7013 (DSN 375)	(301) 225-7228 (DSN 375)	(334) 416-5894 (DSN 596)
Navy/Marine Corps		
(301) 225-7210 (DSN 375)		

MODIFICATIONS TABLE

Date	Version Number	Section Reference	Changed By	Description
4/2009	2.0	Part II	CD27	New
12/2009	3.0	ALL	CD27	Updated throughout
3/2010	4.0	All	CD27	Format & content changes throughout
8/2011	5.0	All	CD27	Reformatted Service Catalog. Content changes throughout.

TABLE OF CONTENTS

1. APPLICATION HOSTING 1
1.1. IBM Mainframe 1
1.2. IBM Mainframe z/Linux 5
1.3. Unisys Mainframe 10
1.4. Server 14
1.5. Storage Support for Server-Based Applications 21
1.6. Continuity of Operations/Service Continuity 26
2. CLOUD SERVICES 32
2.1. Rapid Access Computing Environment 32
2.2. Global Content Delivery Service 34
2.3. System Network Availability Performance System 38
2.4. Forge.mil 40
2.5. Web Hosting Services 42
2.6. Automated Time, Attendance, and Production System 45
3. OTHER IT SUPPORT SERVICES 46
3.1. Data Communications Services 46
3.2. Secure File Gateway Relay Service 50
3.3. Voice and Circuit Support 53
4. SERVICES IN DEVELOPMENT 60
4.1. DoD Enterprise E-Mail 60
4.2. Enterprise SharePoint Service 63
5. ADDITIONAL INFORMATION 66

5.1. DISA CSD Business Model 66

5.2. DISA CSD Inherited IA Controls 67

5.3. Customer Service 74

5.4. DISA CSD Partner Portal 76

5.5. Host-Based Security System 78

5.6. Operating Environment Sizing 80

5.7. Service Desk 82

5.8. Enterprise System Management Software 88

APPENDIX A – ACRONYMS A-1

APPENDIX B – GLOSSARY B-1

APPENDIX C – REFERENCES AND CITATIONS C-1

APPENDIX D – PERFORMANCE STANDARDS D-1

1. APPLICATION HOSTING

The world-class team of technicians in DISA CSD delivers mature and standardized operations processes, centralized management, and partner-focused support. DISA CSD manages all the partner data, including hardware components (computers, storage devices, and networks), software, and labor. DISA CSD provides the stable environment within which our partners' applications can run.

1.1. IBM Mainframe

1.1.1. Description

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

1.1.2. Standard Features

The following services are included in the rates:

- *System Administration*

  Including, but not limited to:

  - Installing, configuring, and maintaining the operating system and core software components
  - Monitoring the operational status of production systems running on DISA CSD's IBM mainframes
  - Managing user accounts at the operating system (OS) level
  - Installing executive software and associated patches
  - Tuning the OS parameters to optimize performance
  - Installing and maintaining the system security environment
  - Ensuring compliance with Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alerts (IAVAs)
  - Monitoring console messages and system logs
  - Scheduling and monitoring backups for system files
  - Resolving referred trouble tickets
  - Developing standard solutions and procedures for the DISA CSD Knowledge Management System in accordance with standard central procedures and guidance
  - Monitoring the environment for any changes that might affect partner production schedules (and notifying our partners of the same)

- Configuring and maintaining the system communications hardware and software including Systems Network Architecture (SNA) and Internet Protocol (IP) configurations
- Installing and maintaining a standard suite of Enterprise System Management (ESM) software DISA CSD uses to monitor and manage the operating environment

- *Security*

  DISA CSD's computing centers benefit from the high level of physical security afforded by being located on military installations. DISA CSD also provides a superior information assurance (IA) environment. In the transition to the DoD IA Certification and Accreditation Process (DIACAP), DISA CSD has accepted Inherited Controls for a wide range of IA responsibilities and functions.

- *Data Communications*

  This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our partners' users around the nation and the world to connect to the partners' data and DISA CSD's computers. Once the request for information leaves the user's locale (base, office building, home, etc.), DISA CSD will handle the traffic and expedite the response back to the user.

- *Enterprise System Management (ESM) Software*

  These are the tools DISA CSD uses to monitor the health and well-being of our partners' information systems and data and to manage problems when, or before, they occur. These tools alert DISA CSD when conditions are favorable for problems to manifest themselves, so DISA CSD can get the appropriate technicians on the scene to resolve any potential problems before they occur.

- *Level 2 Service Desk Support*

- *Storage*

  Storage in the IBM computing environment consists of tape backup and the associated communication infrastructure. IBM storage services are currently billed within one cumulative rate that includes disk and tape. CSD now offers, at a reduced rate, long term tape storage for partners who are required to keep data for long periods of time. To qualify for this rate the data must be older than four-hundred (400) days and written to tape.

- *Assured Computing/IT Service Continuity*

  Our partners that purchase IBM mainframe will receive, at no additional charge, the use of a shared continuity-of-operations processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will automatically be assigned to the partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our partners will be protected by the COOP/Service

Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

- *Mainframe Internet Access Portal (MIAP)*

  MIAP is the DISA CSD standard data transmission tool and will be provided at no additional cost.

- *Capacity Planning*

  Capacity reporting at the logical partition level confirms current resource usage trends. DISA CSD collects and retains this usage data to produce summarized reports for our partners. This is a standard service offering to ensure that DISA CSD mainframes are always robust enough to handle our partners' processing requirements.

1.1.3. Optional Features

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

- *Application Support*

  This feature applies to our partners' production information systems and databases, not to the processing environment's OS or other executive software. The application support function monitors production processing; performs production batch scheduling functions, corrects abnormal terminations (abends) and restarts production runs; processes special requests; coordinates and reports system discrepancies; and initiates corrective actions for system alerts. Using instructions developed by technical support and applications support, applications support personnel manage database and application environments, including recovery procedures.

- *Dedicated Logical Partition (LPAR)*

  When our partner's application runs in a shared partition on a mainframe, the partner will be charged standard mainframe rates. If the partner requires a dedicated partition on a mainframe, that service will be a surcharge to compensate for the inefficiencies.

- *Dedicated IBM Mainframe*

  When our partner's application runs in a shared partition on a mainframe, the partner will be charged standard mainframe rates. If the partner requires an entire dedicated mainframe, that service will be a surcharge to compensate for the inefficiencies.

- *Classified Continuity of Operations (COOP)/Service Continuity*

1.1.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

- *Interactive Availability*

- *Batch Throughput*
- *Job Failure Notification*
- *Data Retrieval*
- *Capacity Utilization*
- *Web-based Invoicing*
- *Optional monitoring using System Network Availability Performance Service (SyNAPS) is available at additional cost*

1.1.5. Service Rates

To find the rates associated with IBM Mainframe Application Hosting support, please refer to the Rate Schedule.

1.1.6. How to Order

Application Hosting Services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

1.1.7. Partner Responsibilities

To see the details behind our partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

1.2. IBM Mainframe z/Linux

1.2.1. Description

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.

What does this mean to our partner? DISA CSD's new 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*

And here's the best part: LOW COST! Our partners save money several ways. First, they pay based on Central Processing Unit (CPU) usage, so this is a true pay-for-what-you-use model. Second, and potentially most attractive, our partners may be able to reduce their software license costs by having many z/Linux operating environments (OEs) on very few mainframe engines. So, if several OEs use the same software (e.g., 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 partner to pay for discrete licenses and maintenance.

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

1.2.2. Standard Features

The following services are included in the rates:

- *System Administration*

  Including, but not limited to:

  - Monitoring the operational status of production systems running on DISA CSD's IBM mainframes
  - Managing user accounts at the OS level
  - Installing executive software, application software, and associated patches
  - Tuning the OS kernel parameters to optimize performance
  - Installing and maintaining the mainframe security environment
  - Ensuring compliance with Security Technical Implementation Guides (STIGs), Security Readiness Reviews (SRRs), and Information Assurance Vulnerability Alerts (IAVAs)

- Monitoring system logs
- Scheduling backups for system files
- Resolving referred trouble tickets

- *Security*

  DISA CSD provides world-class computing centers, all of which benefit from the high level of physical security afforded by being located on military installations. DISA CSD also provides a superior information assurance (IA) environment. In the transition to the DoD Information Assurance Certification and Accreditation Process (DIACAP), DISA CSD has accepted Inherited Controls for a wide range of IA responsibilities and functions.

- *Data Communications*

  This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our partners' users around the nation and the world to connect to the partners' data and DISA CSD's computers. Once the request for information leaves the user's locale (base, office building, home, etc.), DISA CSD will handle the traffic and expedite the response back to the user.

- *Enterprise System Management (ESM) Software*

  These are the tools DISA CSD uses to monitor the health and well-being of our partners' information systems and data and to manage problems when (and sometimes before) they occur. These tools alert DISA CSD when conditions are favorable for problems to manifest themselves, so DISA CSD can get the appropriate technicians on the scene to resolve any potential problems before they occur.

- *Level 2 Service Desk Support*

- *Storage*

  Storage in the IBM z/Linux computing environment consists of tape backup and the associated communication infrastructure. IBM zLinux storage services are currently billed within one cumulative rate that includes disk and tape.

- *Assured Computing/IT Service Continuity*

  Our partners that purchase z/Linux with unclassified processing will receive, at no additional charge, the use of a shared continuity-of-operations processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will automatically be assigned to the partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our partners will be protected by the COOP/Service Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

- *Mainframe Internet Access Portal (MIAP)*

  MIAP is the DISA CSD standard data transmission tool and will be provided at no additional cost.

- *Capacity Planning*

  Capacity reporting at the logical partition level confirms current resource usage trends. DISA CSD collects and retains this usage data to produce summarized reports for our partners. This is a standard service offering to ensure that DISA CSD mainframes are always robust enough to handle our partners' processing requirements

1.2.3. Optional Features

Because our different partners require different levels of support, DISA CSD 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 one of our partners has a uniquely large workload, DISA CSD will work with the partner to develop an agreeable labor support cost method outside of these rates.

- *Database Administration*

  These rates consist of (1) the labor costs of the DBAs supporting any database management systems that run on Linux platforms and (2) the costs of database management tools that improve their productivity. An example of the latter is the Oracle Management Packs, which automate or simplify many labor-intensive tasks.

  The following list identifies some of the functions that DISA CSD DBAs perform on our partners' behalf:

  - Setting up database structures
  - Initial Environment Configuration: physical layout of the database environment and storage allocation
  - Creating or modifying database instances; installing, upgrading, and patching the database software; and adjusting authorizations and permissions of users and groups
  - Complying with STIGs
  - Scheduling database backups and maintaining the procedures for COOP
  - Resolving trouble tickets
  - Availability monitoring (DISA-provided) for database instances.

- *24 x 7 System Administration*

  The z/Linux CPU rate provides for on-site system administration for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site system administration, however, we offer a separate rate to cover the 16 non-prime

shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *24 x 7 Database Administration*

  The standard Database Administration rate provides for on-site database administration for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site database administration, we offer a separate rate to cover the 16 non-prime shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *24 x 7 Application Support*

  The standard Application Support rate provides for on-site application support for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site application support, we offer a separate rate to cover the 16 non-prime shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *Local Operational Recovery*

  In the event of a server failure at the primary processing site, the relevant maintenance program in effect will be the default vehicle for returning the server to production status. If our partners require a greater degree of protection, they may place additional equipment at the production site and have that equipment pre-configured and available to serve as a local fail-over environment.

1.2.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

- *Interactive Availability*
- *Batch Throughput*
- *Job Failure Notification*
- *Data Retrieval*
- *Capacity Utilization*
- *Web-based Invoicing*
- *Optional monitoring using System Network Availability Performance Service (SyNAPS) is available at additional cost.*

1.2.5. Service Rates

DISA CSD will use a z/Linux rate to charge our partners by measuring the number of CPU hours their workloads use. DISA CSD will charge for storage in the z/Linux environment using server storage rates.

To find the rates associated with IBM Mainframe z/Linux Application Hosting support, please refer to the Rate Schedule.

1.2.6. How to Order

Application Hosting Services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

1.2.7. Partner Responsibilities

To see the details behind our partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

1.3. Unisys Mainframe

1.3.1. Description

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

1.3.2. Standard Features

The following services are included in the rates:

- *System Administration*

  Including, but not limited to:

  - Monitoring the operational status of our partners' production systems running on DISA CSD's Unisys mainframes and Test and Development (T&D) platforms
  - Managing user accounts at the operating system (OS) level
  - Installing executive software and associated patches
  - Tuning the OS parameters to optimize performance
  - Installing and maintaining the mainframe security environment
  - Ensuring compliance with Security Technical Implementation Guides (STIGs), Security Readiness Reviews (SRR), and Information Assurance Vulnerability Alerts (IAVAs)
  - Monitoring system logs
  - Scheduling backups for system files
  - Resolving referred trouble tickets

- *Security*

  DISA CSD provides world-class computing centers, all of which benefit from the high level of physical security afforded by being located on military installations. DISA CSD also provides a superior information assurance (IA) environment. In the transition to the DoD Information Assurance Certification and Accreditation Process (DIACAP), DISA CSD has accepted Inherited Controls for a wide range of IA responsibilities and functions.

- *Data Communications*

  This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our partners' users around the nation and the world to connect to the partners' data and DISA CSD's computers. Once the request for information leaves the user's locale (base, office building, home, etc.), DISA CSD will handle the traffic and expedite the response back to the user.

- *Enterprise System Management (ESM) Software*

  These are the tools DISA CSD uses to monitor the health and well-being of our partners' information systems and data and to manage problems when (and sometimes before) they occur. These tools alert DISA CSD when conditions are favorable for problems to manifest themselves, so DISA CSD can get the appropriate technicians on the scene to resolve any potential problems before they occur.

- *Level 2 Service Desk Support*

- *Storage*

  Storage in the Unisys computing environment consists of tape backup and the associated communication infrastructure. Unisys storage services are currently billed based on usage using the current rates.

- *Assured Computing/IT Service Continuity*

  Our partners that purchase Unisys mainframe with unclassified processing will receive, at no additional charge, the use of a shared continuity-of-operations processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will automatically be assigned to the partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our partners will be protected by the COOP/Service Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

- *Mainframe Internet Access Portal (MIAP)*

  MIAP is the DISA CSD standard data transmission tool and will be provided at no additional cost.

- *Capacity Planning*

  Capacity reporting at the logical partition level confirms current resource usage trends. DISA CSD collects and retains this usage data to produce summarized reports for our partners. This is a standard service offering to ensure that DISA CSD mainframes are always robust enough to handle our partners' processing requirements

1.3.3. Optional Features

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

- *Application Support*

  This feature applies to our partners' production information systems and databases, not to the processing environment's operating system or other executive software. The application support function monitors production processing; corrects abnormal terminations (abends) and restarts production runs; processes special requests; coordinates and reports system discrepancies; and initiates corrective actions for

system alerts. Using instructions developed by technical support and applications support, applications support personnel manage database and application environments, including recovery procedures. The rate consists of the labor costs of the technicians.

- *Dedicated Logical Partition (LPAR)*

  When our partner's application runs in a shared partition on a mainframe, the partner will be charged standard mainframe rates. If our partner requires a dedicated partition on a mainframe, that service will be a surcharge to compensate for the inefficiencies.

- *Dedicated Unisys Mainframe*

  When our partner's application runs in a shared partition on a mainframe, the partner will be charged standard mainframe rates. If our partner requires an entire dedicated mainframe, that service will be a surcharge to compensate for the inefficiencies.

- *Classified Continuity of Operations (COOP)/Service Continuity*

1.3.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

- *Interactive Availability*
- *Batch Throughput*
- *Job Failure Notification*
- *Data Retrieval*
- *Capacity Utilization*
- *Web-based Invoicing*
- *Optional monitoring using System Network Availability Performance Service (SyNAPS) is available at additional cost.*

1.3.5. Service Rates

To find the rates associated with Unisys Mainframe Application Hosting support, please refer to the Rate Schedule.

1.3.6. How to Order

Application Hosting Services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

1.3.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

1.4. Server

1.4.1. Description

The unit of measure for Basic Services is the operating environment (OE), which DISA CSD defines as an instance of an operating system (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 central processing units (CPUs) will determine the size of the OE (Level 2 to 6). The rates differ based on size and OS.

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

1.4.2. Standard Features

The following services are included in the rates:

- *System Administration*

  Including, but not limited to:

  - Monitoring the operational status of our partners' production systems running on DISA CSD's Windows, Linux, and Unix servers
  - Managing user accounts at the OS level
  - Installing executive software, application software, and associated patches
  - Tuning the OS kernel parameters to optimize performance
  - Installing and maintaining the server security environment
  - Ensuring compliance with Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alerts (IAVAs)
  - Monitoring system logs
  - Scheduling backups for system files
  - Resolving referred trouble tickets

- *Security*

  DISA CSD provides world-class computing centers, all of which benefit from the high level of physical security afforded by being located on military installations. DISA CSD also provides a superior information assurance (IA) environment. In the transition to the DoD Information Assurance Certification and Accreditation Process

(DIACAP), DISA CSD has accepted Inherited Controls for a wide range of IA responsibilities and functions.

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

1.4.3. Optional Features

Because each of our partner's processing requirements may differ from the next partner, DISA CSD offers all our 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*

  This rate is required if DISA CSD owns or maintains the servers (OEs), including hardware that DISA CSD acquires from its capacity services contracts.

  The Hardware Services rate covers the cost of DISA CSD provided hardware, OS software, standard maintenance, and miscellaneous items such as racks and cabling. In most cases this is hardware provided by DISA CSD's capacity vendors. For legacy hardware, this rate covers the cost of depreciation.

  Capacity planning and reporting are also included in the Hardware Services rate. Capacity reporting at the OE level confirms current CPU and memory resource usage trends. DISA CSD collects and retains all this usage data to produce summarized reports for our partners. This is a standard service offering to ensure that DISA CSD servers are always robust enough to handle our partners' processing requirements. If our partners maintain their own hardware, and thus do not pay the Hardware Services rate, they may avail themselves of capacity planning and reporting at a cost of 10 percent of the Hardware Services rate for their suite of hardware.

  Please note that when our partners pay the Hardware Services rate, whether for their servers or DISA CSD servers, they automatically qualify for periodic technical refresh at no additional cost. DISA CSD will obtain OEs from capacity services to replace the partner's old servers when the time comes for a technical refresh. Our partners do not have to worry about hardware acquisition or budgeting for capital funds for IT replacements. DISA CSD will do it for them.

- *Application Support*

  This feature pertains to our partners' production information systems and databases, not to the processing environment's OS or other executive software. The application support function monitors production processing; corrects abnormal terminations (abends), and restarts production runs; processes special requests; coordinates and reports system discrepancies; and initiates corrective actions for system alerts. Using instructions developed by technical support and DISA CSD's applications support, applications support personnel manage database and application environments, including recovery procedures.

The application support rates consist of the labor costs of the technicians performing the functions listed above, as well as the following tasks:

- Changing disk space allocation as required
- Resolving job aborts and other errors during processing
- Building, maintaining, and monitoring job schedules
- Coordinating with the database administrators (DBAs) and system administrators (SAs) on new and/or changed releases
- Associating security profiles to jobs
- Monitoring backups
- Mitigating contention and/or improving application performance
- Coordinating with our partners on service interruptions
- Managing, coordinating, and installing application releases
- Managing reports (for example, using software such as CA-Dispatch)
- Reviewing and monitoring system or application logs as required by SLAs
- Creating and setting up user account profiles in required applications and databases (in some situations and for some workloads)

- *Web Administration*

  Web administration refers to the labor to administer a web server and its associated software. Web administration does not include creating or designing web sites. Nor does it apply to managing the content on the web servers. DISA CSD web administrators do the following:

  - Set up and maintain web servers
  - Coordinate with partner support staff involved in putting together and maintaining web sites
  - Write reports and analyze web site user statistics
  - Repair system-related problems that may occur
  - Provide user support

  This service only applies to the OEs that are functioning as web servers, and not to application servers, database servers, domain name servers, etc. If a web server uses Microsoft's Internet Information Services (IIS) software, then DISA CSD will provide this service at no additional charge. (For IIS only, this service is included in the Basic Services rate.) Because we cannot share system-level access to Windows OEs, web administration is a mandatory charge for all Windows-based web servers that use web software other than IIS. Web administration is optional for all Unix and Linux OEs.

- *Database Administration*

  These rates consist of (1) the labor costs of the DBAs supporting any database management systems that run on Unix or Windows platforms and (2) the maintenance costs of database management tools that improve their productivity. An example of the latter is the Oracle Management Packs, which automate or simplify many labor-intensive tasks.

  The following list identifies some of the functions that DISA CSD DBAs perform on our partner's behalf:

  - Setting up database structures
  - Allocating space
  - Creating or modifying database instances
  - Complying with Security Technical Implementation Guides (STIGs)
  - Scheduling backups for data files
  - Resolving trouble tickets
  - Developing standard procedures for the DISA CSD Knowledge Management System, based on the proclivities of the information system and its associated databases

  If our partners serve as their own DBAs, DISA CSD must still ensure that their databases comply with the DoD's security guidelines. The charge for this service is 10 percent of the full Database Administration rate per database OE. The security fee includes the following services:

  - Consultative services on the STIG
    - Consulting is defined as providing STIG interpretation and clarification to our partners. Consulting does not include performing Vulnerability Management System (VMS) data entry.
    - Assist partners in entry and validating VMS
      - Our partners have the responsibility to perform VMS functions
        - System/Enclave creation
        - VMS Reports
        - Plan of Action and Milestones (POA&M) entry
        - Designated Approving Authority (DAA) Risk Acceptance (DRA) entry
        - Update findings to proper status (Fixed, Open, Not a Finding, etc.)
        - Etc.

- CSD will provide instruction in the use of VMS
  - System/Enclave creation
  - How to run VMS reports
  - How to input POA&Ms and DRAs
  - How to update findings
  - Etc.

- Answer questions about how to handle STIG findings with respect to database requirements
  - This is defined as interpreting database STIG requirements.
  - If CSD is unable to interpret STIG requirements, CSD will provide our partners with FSO Support information.
- Scanning the databases, and provide output to partners for resolution.

(Note that if DISA CSD is serving as the partners' DBAs, there is no security surcharge as it is included in the Database Administration rate.) Finally, for any OEs that use Oracle Application Server (OAS), DISA CSD charges only 50 percent of the Database Administration rate per OAS OE.

DISA CSD's DBAs use Oracle Enterprise Manager (OEM) Grid Control to manage our partners' databases. OEM Grid Control is a collection of utilities that automates a variety of time-consuming tasks, allowing the DBAs to use their time more productively. DISA CSD's partners who pay the full Database Administration rate on their database OEs receive the full benefit of these tools (additionally, the database security is included in the full Database Administration rate). For example, the Database Administration rate includes the costs of the DBA's labor, as well as the maintenance costs of the OEM Grid Control software that DISA CSD's DBAs use.

For those partners who use their own DBAs and would like their DBAs to use DISA CSD's OEM Grid Control software, they may pay an additional 10 percent to cover the cost of the software.

- *Oracle Database Software Maintenance*

  The Oracle database management system is the most prevalent database application among the DISA CSD partner community. To that end, DISA CSD has established a rate for Oracle database software. This rate consists of the maintenance costs of the Oracle database software only. (The license fee for Oracle is charged as a one-time implementation cost. Also, the costs of other database management systems are considered cost-reimbursable and are not covered by these rates.)

- *24 x 7 System Administration*

  The Basic Services rate provides for on-site system administration for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site system administration, however, we offer a separate rate to cover the 16 non-prime shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *24 x 7 Database Administration*

  The standard Database Administration rate provides for on-site database administration for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site database administration, we offer a separate rate to cover the 16 non-prime shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *24 x 7 Application Support*

  The standard Application Support rate provides for on-site application support for five eight (8) hour shifts weekly (e.g., Monday through Friday from 0800 to 1600). It also includes a two (2) hour response to emergencies on nights and weekends and on-site support for the monthly scheduled maintenance window. For those workloads requiring 24x7 on-site application support, we offer a separate rate to cover the 16 non-prime shifts. This provides for immediate response to an emergency 24 hours a day, seven (7) days a week.

- *Cost-Reimbursable (Non-Rate) Services*

  Because DISA CSD hasn't established rates for every conceivable service a partner may request, unique requests are handled on a cost-reimbursable basis. For these offerings, DISA CSD charges the direct cost, plus all indirect and general and administrative costs. This list represents some of the cost-reimbursable services provided to our partners, but it is far from exhaustive.

  - Non-standard OS's, such as Tandem Guardian, DEC VAX, or anything else other than Windows, Linux, or Unix
  - Unique communications requirements such as Virtual Private Networks (VPNs), community of interest networks, Demilitarized Zones (DMZs), dedicated circuits, dedicated enclaves, etc.
  - Certain test, development, or training environments that are not conducive to rates
  - Database monitoring, including the license and maintenance costs of requisite software tools
  - Process-improvement teams dedicated to resolving complex issues across disparate hardware and/or software platforms

  - Software development
  - Commercial, off-the-shelf (COTS) software that is ancillary to, but required for, the information system to work properly
  - Certain non-standard, partner-owned servers that DISA CSD maintains
  - Certain extremely large OEs that would skew the rates if left within the rates
  - Subject matter experts who provide specific, in-depth knowledge of a COTS software product (e.g., SAP, McAfee's ePolicy, Oracle's Service-Oriented Architecture software, etc.)
- *Continuity of Operations (COOP)/Service Continuity*

1.4.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

- *Interactive Availability*
- *Batch Throughput*
- *Job Failure Notification*
- *Data Retrieval*
- *Capacity Utilization*
- *Web-based Invoicing*
- *Optional monitoring using System Network Availability Performance Service (SyNAPS) is available at additional cost.*

1.4.5. Service Rates

To find the rates associated with Server Application Hosting support, please refer to the Rate Schedule.

1.4.6. How to Order

Application Hosting Services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

1.4.7. Partner Responsibilities

To see the details behind our partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

1.5. Storage Support for Server-Based Applications

1.5.1. Description

Our partners purchasing Server services are offered a wide array of storage opportunities that allow DISA CSD to provide the level of service required for all MAC levels.

Rate-based server storage pricing is based on the GB (raw) storage used per month and the level of service requested by the partner for data recovery, not application restoration based on Recovery Time Objective (RTO) and Recovery Point Objective (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 tapes to recover on existing production storage capacity. Entries L2, L3 and L4 are advanced local data recovery options. Please note that local recovery will not satisfy the Continuity of Operations (COOP)/Service Continuity requirements detailed in DoD Instruction 8500.2, which mandates a remote recovery strategy at a predetermined location.

Level	MAC Level	Description	Maximum Data Loss
L1	MAC III	Default Local	7 Days
L2	MAC II	Operational Local	24 Hours
L3	MAC II	High-Availability Local	8 Hours
L4	MAC I	Non-Disruptive Local	1 Second

1.5.2. Standard Features

- *Default Local/Operational Recovery (L1)*

  This offering includes only local/operational recovery following an outage at the primary production/processing site. The offering assumes that the hardware and software elements of the processing environment are, or can be made, operational and that data backups can be used to restore the application.

  Our partners will be invoiced for all appropriate costs based on the service selected and the amount of allocated storage in gigabyte (GB)/month. All partners will be provided and invoiced the Basic Service Level L1 in the table below for data recovery, not application restoration. Partners may select to augment the Basic Service in accordance with their needs and MAC level. If a partner chooses to buy only basic storage for a server application that may have a higher MAC level, thus a need for remote recovery, it will be noted in Section 7.0 of the SLA.

Level	MAC Level	Description	Maximum Data Loss
L1	MAC III	Basic/Default Local	24 Hours to 1 Week
Hardware		Depreciation and Maintenance	
		Infrastructure – switches, backup media	
		Racks, cables	
Software		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	

1.5.3. 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)*

  This level of continuity provides sufficient storage infrastructure in place to allow an operational recovery with a maximum data loss of 24 hours. The reduced timeline is driven by the use of on-site storage capacity, which maintains data backups in a near online state. This advanced level of recovery does not require a corresponding server element in order to be effective; it assumes that the production server infrastructure is in place and usable. However, it may be augmented by local additional processing capability as well.

- *High-Availability Local/Operational Recovery Combination 2 (L3)*

  This level of continuity provides sufficient storage infrastructure in place to allow an operational recovery with a maximum data loss of eight (8) hours. The reduced timeline is driven by the use of on-site storage capacity, which maintains data backups in an online state and creates/captures backups on a more frequent basis. This advanced level of recovery does not require a corresponding server element in order to be effective; it assumes that the production server infrastructure is in place and usable. However, it may be augmented by local additional processing capability as well.

- *Non-Disruptive Local/Operational Recovery Combination 3 (L4)*

  This level of continuity provides sufficient storage infrastructure in place to allow an operational recovery with a maximum data loss of less than one (1) second and an RTO of 30 minutes. The reduced timeline is driven by the use of data replication to create near-instantaneous backups.

  NOTE: For this advanced level of recovery to be effective, a corresponding hardware and software infrastructure needs to be available and operational at the primary production site. This approach is also referred to as "local failover," and is designed to ensure minimal data loss and relatively minimal interruption in data processing.

  The infrastructure can be set up with a standard failover process, meaning the infrastructure is not operational until needed in response to an outage experienced by the primary processing platform; or it can be set up in a "workload balancing" configuration. Workload balancing would allow for both the primary and the fail-over equipment to be used simultaneously. If one half of the infrastructure is affected by an outage, the other half is sufficiently sized and configured to take on the entire workload.

  The various approaches used to implement this advanced option would be negotiated, and priced, as part of the development and defining of the SLA requirements.

- *Cost Reimbursable Services*
  - More copies and longer retention of weekly and incremental backups beyond established basic service
  - Additional application backups
  - Additional or special offsite storage services
  - Special Advanced Functionality
    - Encryption of data at rest and/or in transit
    - Content addressable storage

Overview of Local Recovery options

Options	MAC Level	Description	Maximum Data Loss
Local/Operational Recovery	Typically used for MAC III applications	Recovery in place using production equipment and backup data	7 Days
Advanced Local/Operational Recovery Combination 1	Typically used for MAC II applications	Recovery in place using production equipment and backup data in a near-online state	24 Hours
Advanced Local/Operational Recovery Combination 2	Typically used for MAC II applications	Recovery in place using production equipment and frequently updated backup data in a near-online state and/or designated remote site	8 Hours
Advanced Local/Operational Recovery Combination 3	Typically used for MAC I applications	Recovery in place using synchronous replicated data maintained on-site and utilizing sufficient pre-configured processing infrastructure to host the restored system(s)	1 Second

NOTE: DoD 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.

1.5.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

Optional monitoring using System Network Availability Performance Service (SyNAPS) is available at additional cost.

1.5.5. Service Rates

To find the rates associated with Server-based storage support, please refer to the Rate Schedule.

1.5.6. How to Order

Application Hosting Services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

1.5.7. Partner Responsibilities

To see the details behind our partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

1.6. Continuity of Operations/Service Continuity

1.6.1. Description

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

For mainframe processing, including z/OS, z/Linux*, and Unisys platforms, the cost of COOP/Service Continuity is included in the rates (*additional storage cost applies). For all server-based processing, the basic rates do not include this coverage. Our partners with server-based processing must “opt in” to the COOP program by specifically selecting and paying for the appropriate remote recovery protection. Our partners who purchase Server services but do not purchase COOP services from DISA CSD will need to satisfy the requirement through the use of in-house or third party resources.

It is DISA CSD’s policy that COOP will only be offered for those applications where DISA already has the production processing requirement. DISA CSD will not pursue or accept "COOP Only" arrangements for processing.

All storage solution programs used by DISA CSD for data replication as well as tape-based backups are designed to serve multiple partners. It is possible that a partner may require unique individual backups to be used in a remote recovery by parties other than DISA CSD; however, in these situations, the standard backup approach is not designed to satisfy this requirement. While not a COOP service, the partner may contract with DISA CSD for the creation of application specific backups; however, the partner will be responsible for reimbursing DISA CSD for the associated cost.

1.6.2. Standard Features

COOP/Service Continuity consists of the policies, procedures, and programs that allow DISA CSD, 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.

The continuity-related IA controls from DoDI 8500.2 are listed below and are satisfied by the COOP program as overseen by DISA CSD.

Control	Mitigation Strategy
Alternate Site Designation	An alternate site is identified as a recovery location and has appropriate equipment and infrastructure to allow restoration of processing capability.
Protection of Recovery Assets	Procedures exist to ensure the physical and technical protection of recovery infrastructure.

Data Backup Procedures	Data is backed up according to the required frequency and stored off-site.
Disaster and Recovery Planning	Plans and procedures exist to allow resumption within required time frames.
Enclave Boundary Defense	Measures in place are similar to production site protections.
Scheduled Exercises and Drills	Annual exercises are available upon partner request.
Identification of Essential Functions	Where identified by the partner, mission essential functions and their supporting assets are considered in determining restoration priorities.
Maintenance Support	Maintenance support for key IT assets can respond within required timeframes.
Power Supply	Uninterruptible Power Supply (UPS) and emergency generator protection is in place.
Spares and Parts	Maintenance spares and parts for key IT assets can be obtained within required timeframes.
Backup Copies of Critical Software	Backup copies of critical software are maintained offsite.
Trusted Recovery	Procedures exist to ensure a secure and verifiable recovery effort.

For partners purchasing IBM and Unisys mainframe processing, there is an Assured Computing Environment (ACE) approach to providing COOP that will meet MAC II requirements (processor and data) for remote recovery. This approach is included in the standard rates for those services. For z/Linux on the IBM mainframe, the rate includes the processing capacity and capability; however, an additional charge for the storage component of the recovery infrastructure is required.

Server-based processing does not include COOP/Service Continuity in the basic rates and requires the partner to specifically select and pay for the desired and compliant coverage (see Optional Features)

DISA CSD, in concert with partner personnel, will take the lead in developing, maintaining and updating recovery procedures. However, the creation of recovery procedures will only be accomplished for those applications for which DISA has a defined and documented recovery responsibility. Procedures designed to be used by an alternate provider or by the partner utilization of their own internal resources will have to be developed by those responsible for the recovery and familiar with the supporting infrastructure for the planned recovery.

DISA CSD will allow auditors, working through the CSD CIO office, to review documentation associated with satisfying COOP-related IA controls. For security purposes, specific recovery documentation will not be distributed to the auditors; however, an Audit Artifact package will be provided as documented evidence of IA Control compliance.

When contracting with DISA for COOP/Service Continuity, the partner can request exercises of that coverage using the processes and/or environments that would be used for an actual recovery. The two primary types of exercises are tabletop and simulation. There is no additional charge to the partner to conduct these exercises; however, they are limited to no more than one per year. The first exercise for either new workloads or workloads that have undergone major updates or changes to the operating environment (OE) will be conducted as a tabletop. After that the partner will be eligible for a simulation every three years with tabletop exercises in between.

In a tabletop exercise, the personnel who would be involved in an actual recovery gather together and walk through the processes developed for that recovery. The time to complete a tabletop exercise will be dependent on the scope and coordination requirements associated with the exercise. Typically, these exercises are conducted within an hour. The minimum planning lead time before a tabletop can be conducted is 45 days.

In a simulation exercise, the application or applications in question are physically recovered at their pre-designated recovery site using the recovery procedures in the Business Continuity Plan (BCP) for the production site. The time to complete such an exercise will be dependent on the scope and coordination requirements associated with the exercise as well as the environment at the designated recovery site(s). Typically, these exercises will be two to three weeks in length. The minimum planning lead time before a simulation can be conducted is 90 days.

1.6.3. 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	RTO = 5 Days 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 Hrs
RRC 2	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured, and operational processing capability at the designated recovery site	Operational Remote	Dedicated COOP	RTO & RPO = 24 Hrs
RRC 3	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured, and operational processing capability at the designated recovery site	High-Availability Remote	Dedicated COOP	RTO & RPO = 8 Hrs

Option	MAC Level	Description	Storage Offering	Processor Offering	RTO/RPO
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.

If the partner determines that the pre-defined approaches are not adequate or preferred, then a custom solution can be developed and implemented (Failover, Test and Development (T&D), partner-managed, etc.). Any solution of this type must be identified within the relevant SLA. In addition, any supporting documentation must be appended to or referenced within that SLA. For partner-managed solutions where the partner is responsible for facilitating their own exercises and maintaining their own documents to support regulatory requirements, they are still required to follow the Exercise Restrictions & Guidance policy with regard to scheduling and site coordination.

1.6.4. Service Performance

DISA CSD shall make a good faith effort to meet or exceed the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) associated with any selected or included COOP offering. Recovery procedures and infrastructure will be developed and implemented with the intent of meeting those targets and exercises will be designed and conducted with the goal of verifying that capability.

1.6.5. Service Rates

DISA CSD operates financially as a Defense Working Capital Fund (DWCF) business entity. As such, CSD is required to recover all costs of operations through billing for services provided. To the maximum extent possible, CSD develops rates, approved by the DoD Comptroller, to assign cost to services.

To find the rates associated with COOP/Service Continuity coverage, please refer to the Rate Schedule.

1.6.6. How to Order

COOP/Service Continuity coverage and support provided by CSD can be obtained by working with a CSD CME Team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

1.6.7. Partner Responsibilities

To successfully integrate an application into the COOP/Service Continuity program, there are certain responsibilities which cannot be performed by CSD, including:

- *Paying for the CSD support*
- *Having a DIACAP-ready application with a partner DAA ATO, etc.*
- *Initiating requests for COOP capability exercises through the assigned Customer Account Representative (CAR). (Exercises are not conducted unless there is a partner request and partner involvement in the verification and validation of the recovery exercise effort.)*
- *Initiating termination or removal of COOP coverage for server-based processing*

Also, exercises of COOP capability require an initiating request from the partner through their assigned CAR.

NOTE: Any partner who is not contracting with DISA CSD for COOP/Service Continuity services is specifically excluded from the DISA program. No promise or expectation of COOP/Service is implied or should be inferred. The SLA will include an annotation that the partner has "No DISA-provided COOP" requirements that are to be satisfied by DISA CSD.

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2. CLOUD SERVICES

Cloud Computing is a means of enabling convenient, on-demand network access to a shared pool of configurable computing resources (i.e. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The DISA CSD cloud model promotes availability and continuous integration, and is defined by five essential characteristics supporting one initial delivery model.

2.1. Rapid Access Computing Environment

For more details, please visit http://disa.mil/race/.

2.1.1. Description

The Rapid Access Computing Environment (RACE) service provides a streamlined process for the provisioning and subsequent development; testing; and through the utilization of Enterprise Mission Assurance Support Service (eMASS) and Vulnerability Management System (VMS), streamlined certification, accreditation and deployment of applications to a DISA Defense Enterprise Computing Center (DECC). DISA CSD packages hosting, networking, security and connectivity together as a service. 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.

2.1.2. Standard 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 (7) to 10 days.

2.1.3. Optional Features

Please visit the http://disa.mil/race/ for additional information.

2.1.4. Service Performance Levels

Development and test environments are available within 24 hours of receipt of payment. Production environments are available within seven (7) to 10 days of receipt of payment and completion of Certification and Accreditation (C&A) paperwork.

2.1.5. Service Rates

To find the rates associated with RACE support, please refer to the Rate Schedule.

2.1.6. How to Order

RACE services can be ordered and paid for directly on the RACE portal at http://disa.mil/race/.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

2.1.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2.2. Global Content Delivery Service

For more details, please visit http://www.disa.mil/gcds/.

2.2.1. Description

The Global Content Delivery Service (GCDS) provides a Defense Information Systems Network (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 (NIPRNet & SIPRNet). 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.

The technology behind the GCDS leverages proprietary routing algorithms that dynamically and optimally route traffic across the DISN, even as network conditions change. GCDS provides services to end users at the edge of the DISN including network optimization featuring:

- *Transmission Control Protocol (TCP) optimization*

  One of the core protocols of the Internet Protocol Suite

- *Object pre-fetching*

  A method that can expedite the presentation of web pages by utilizing the current web page's view time to acquire the web objects of future web pages

- *Persistent connections*

  Links that do not close when the execution of a web page script ends

- *Secure Socket Layer (SSL) off-load*

  Procedure transfers a portion of SSL processing duties, normally handled by servers, to a separate, specially designed device

- *Content delivery services such as:*
  - Caching – a process that greatly increases the speed at which a computer pulls bits and bytes from memory
  - Data compression – the process of encoding information using fewer bits than the original representation would use
  - Failover – the capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active application, server, system, or network

- *Reporting and monitoring services such as traffic reports and alerts.*

  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). All our partners purchasing GCDS are provided 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 to our GCDS partners 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 the partner's origin site and GCDS (two transactions). If the partner wants additional transactions, they can be purchased separately.

2.2.2. Standard Features

DISA CSD, as an agent for DISA and responsible party for program management of GCDS, will plan the deployment logistics, expected service levels, and other program specific criteria. The managed service provider will provide the servers to DISA CSD 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*
  - This will include hardware, software, firewall, and circuit deployments to upgrade the infrastructure used in GCDS.
- *Professional services, integration services, and partner care (including service desk)*
  - The managed service provider for GCDS will provide secret cleared personnel on-site to perform these functions and additionally to train DISA CSD personnel in the performance of these functions.
- *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.

2.2.3. Optional Features

- *GCDS NetStorage*

One of the main goals of DoD organizations providing mission critical content on the NIPRNet or SIPRNet 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, our partners can make their rich media content available to users on demand, anytime and anywhere.

2.2.4. Service Performance Levels

- *Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA)*
- *Quarterly Customer Performance Assessments*
- *The GCDS Portal provides the ability for users to:*
  - Purge Content from GCDS
    - A purge will delete all of the content forward deployed into the GCDS. Before the users can experience the efficiencies of the GCDS, the network must be re-populated with the data under the purged URL.
  - Configure Log Delivery Service
  - View reports
  - Produce reports for kilobytes per second and hits (number of access attempts to a web site) per second
  - Configure alerts
    - Edge Errors
    - High Traffic
    - Incomplete Downloads

- Low Traffic
- Origin Access Denied
- Origin Connection Failures
- Origin DNS Failures
- Origin Object Not Found
- Origin Server Failure
- Origin SSL Transaction Failure

2.2.5. Service Rates

To find the rates associated with GCDS support, please refer to the Rate Schedule.

Note: GCDS transitions into the DISN Subscription Service (DSS) in October FY12. This means that partners on GCDS in FY11 will no longer be billed monthly recurring charges in FY12.

2.2.6. How to Order

GCDS services are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

2.2.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2.3. System Network Availability Performance System

For more details, please visit http://www.disa.mil/gcds/features.html.

2.3.1. Description

System Network Availability Performance Service (SyNAPS), utilizing 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 and between 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.

2.3.2. Standard 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.

Our partners that purchase SyNAPS 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).

2.3.3. Optional Features

Not Applicable

2.3.4. Service Performance Levels

SyNAPS shall make a good faith effort to meet or exceed our partners' objectives. Circumstances beyond SyNAPS control (i.e. commercial power outages, natural disasters, etc.) are excluded. SyNAPS maintains Mission Assurance Category (MAC) III Classified

confidentially level and will take prompt corrective action when these objectives are not being met.

2.3.5. Service Rates

To find the rates associated with SyNAPS support, please contact your CSD CME team.

2.3.6. How to Order

SyNAPS services are obtained by working with your CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

2.3.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2.4. Forge.mil

For more details, please visit http://www.forge.mil/.

2.4.1. Description

Forge.mil 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.

2.4.2. Standard 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*

2.4.3. Optional Features

For additional information, please visit http://www.forge.mil/.

2.4.4. Service Performance Levels

Not Applicable

2.4.5. Service Rates

Not Applicable (There is no charge for this service.)

2.4.6. How to Order

Forge.mil services are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

Coming Soon – Online Ordering!

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

2.4.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2.5. Web Hosting Services

2.5.1. Description

DISA CSD can provide three levels of web hosting ranging from "simple" to "complex." The standard services are based on the use of Microsoft Windows Std/IIS or Linux/Apache on DISA CSD-provided hardware. WEB Hosting service offerings include MAC III remote recovery. The offerings are summarized as follows:

- *Bronze*

  Simple to intermediate-sized web sites, with CSD-supported scripting and small data requirements (less than one [1] GB per site)

- *Silver*

  Intermediate-sized web sites requiring a dedicated operating environment(s) (OE), scripting support, and increased storage requirements (five [5] 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.

2.5.2. Standard Features

All Web Hosting Levels include the following services:

- *Project Management*
- *Basic services*
- *Systems Administration (SA)*
  - Touch labor, managing system resources and their performance, ensure compliance with Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alerts (IAVAs), resolve referred trouble tickets, etc.
  - Service Desk Support
  - 24/7 Support
  - Off-site storage
  - Network Monitoring
  - Enterprise System Management (ESM)
  - Depending upon the needs of the partner, the ESM tools which may be used for either Windows or Linux environments include:
    - Veritas Netbackup

        - Tivoli for system performance monitoring
        - BladeLogic agents
        - MacAfee
    - Microsoft IIS for Windows
    - Communications Infrastructure
- *Hardware Services*
    - Installation, maintenance, repair, tech refresh
- *Information Assurance (IA)*
    - IAVAs, STIGs, Scans (Retina etc.), Demilitarized Zone (DMZ)
- *Facility Environmentals (Heating, Ventilating, and Air Conditioning [HVAC]; power; Uninterruptible Power Supply [UPS])*
    - N+1 redundancy

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

- *Microsoft SQL Server*
    - Supported on a Windows OE
    - Databases with low Input/Output (I/O) requirements
    - Includes Hardware Services
    - Includes Database Administration
    - Provides High Availability provided by local failover
    - Storage charged at the DISA published per/GB annual rate (MAC III)
- *MySQL*
    - Supported on a Red Hat Linux OE
    - Databases with low I/O requirements
    - Includes Hardware Services
    - Includes Database Administration
    - Provides High Availability provided by local failover
    - Storage charged at the DISA published per/GB annual rate (MAC III)

2.5.4. Service Performance Levels

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

2.5.5. Service Rates

To find the rates associated with Web Hosting support, please contact your CSD CME team.

2.5.6. How to Order

Web Hosting services are obtained by working with your CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

Coming Soon – Online Ordering!

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

2.5.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

2.6. Automated Time, Attendance, and Production System

2.6.1. Description

The Automated Time, Attendance and Production System (ATAAPS) 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 the payroll data to the DoD payroll system. DISA CSD provides partner communities within the federal government unique application support and Service Desk services, currently supporting over 83,779 user accounts.

2.6.2. Standard Features

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

2.6.3. Optional Features

Not Applicable

2.6.4. Service Performance Levels

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

2.6.5. Service Rates

To find the rates associated with ATAAPS support, please refer to the Rate Schedule.

2.6.6. How to Order

ATAAPS services are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

Coming Soon – Online Ordering!

To obtain contact information for your CME team or a SLM Hotline, please refer to the Points of Contact section.

2.6.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

3. OTHER IT SUPPORT SERVICES

3.1. Data Communications Services

3.1.1. Description

DISA CSD has network monitoring tools at its disposal to provide outstanding service for our partners. It is the joint responsibility of DISA Network Services (NS) and DISA CSD to provide and maintain the Global Information Grid (GIG) utilized by our partners. DISA CSD network operations support is provided by a 24x7 staff responsible for identifying and resolving network problems, upgrading network devices and change management. Non-classified Internet Protocol Routing Network (NIPRNet) and Secured Internet Protocol Network (SIPRNet) availability is built into the system via hardware and circuit diversity throughout the Wide Area Network (WAN).

DISA CSD 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 CSD hosts DoD DMZ access nodes and DoD DMZ extensions that provide partners the ability to secure their applications in accordance with the DoD DMZ STIG.

3.1.2. Standard Features

The communications component is comprised of the DISA CSD 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 CSD's processing centers.

NOTE: Partner-specific communications enclaves, community-of-interest networks, virtual private networks, etc., are cost-reimbursable and are not part of the CSD communications infrastructure.

- *Data Transmission Options*

  DISA CSD 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 VPNs	Varies	N/A
.com → .mil (DECC)	B2B	Complete Business to Business (B2B)/VPN checklist and follow instructions enclosed.

Traffic Flow	Solution to Use	Notes
.mil → .mil (DECC)	Policy-Based Co-Location (PB Collo)	If the partner is collocated at DMZ, use partner VPN equipment. If the partner is not collocated at DMZ, use DISA provided VPN. Complete B2B/VPN checklist and follow instructions enclosed.
.mil (DECC) →.mil (DECC)	Inter-DECC VRF	No configuration needed
CSD 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	N/A
Ports 20,21 – FTP (User initiated)	MIAP	Complete MIAP application online at https://miap.csd.disa.mil
Ports 20,21 – FTP (Batch initiated)	B2B or PB Collo & GEX (on the backside)	Complete B2B PB Collo checklist as well as the Global Exchange (GEX) checklist
Port 22 – SSH/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 – HTTP	Web Proxy	Complete WebDMZ checklist
Port 443 – HTTPS/SSL	Web Proxy	Complete WebDMZ checklist
Port 1414 – MQ Series	GEX	Complete GEX
.mil (DECC) → .com or .mil on 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.

NOTE: To obtain any of the checklists referenced in the above table, contact your CME team referenced in the Points of Contact section.

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*

  The DoD B2B is intended to provide a controlled and secure communications portal for authorized contractors, vendors, and other support resources to access non-web based DoD legacy systems and applications as required for mission-critical business and e-commerce activities between .com and .mil. The DMZ Non-Proxy Gateway is similar to the B2B Gateway but is for .mil to .mil traffic. The DoD B2B and Non-Proxy Gateways are designed to require and enforce the use of encryption and mandatory authentication from within the gateway.

- *Web DMZ*

  The Web DMZ infrastructure is designed to support Internet access to all production system applications (such as Internet accessible personnel, medical and informational sites and electronic commerce portals) that use web-based Transmission Control Protocol (TCP) Internet Protocols (IP) (currently HTTP port 80 and HTTPS port 443) with partners in WAN. It also services Domain Name Server (DNS) resolution requests on User Datagram Protocol (UDP) port 53. This infrastructure is intended only for web applications which require back-end NIPRNet connections, for example, database and application server access. It is not intended for web applications with embedded static content, which can be hosted elsewhere (i.e. the Defense Technical Information Center [DTIC]).

3.1.3. Optional Features

Not Applicable

3.1.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

3.1.5. Service Rates

To find the rates associated with Communications Services support, please contact your CSD CME team.

3.1.6. How to Order

Communications services are obtained by working with your CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

3.1.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to the CSD Terms & Conditions document.

3.2. Secure File Gateway Relay Service

3.2.1. Description

The DISA 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.

3.2.2. Standard Features

- *Security*
  - Transitions of any "in the clear" *(e.g. FTP)* data transfers to any FIPS 140-2 certified in-flight encryption.
  - Provides for FIPS 140-2 certified encryption at-rest, both during and post data transference.
  - Both supports and promotes "per user" Public Key Encryption (PKE)/Public Key Infrastructure (PKI) authentication and validation capabilities.
  - Enables PKE/PKI enforcement between each enclave having an SFG Relay Service.
  - Centralizes data transfer routing, for complete auditing and Intrusion Detection System (IDS) coverage.
  - Allows data integrity and anti-virus security checks on a per-file basis
  - Information Assurance (IA)
- *Administration*
  - Consolidates all file transfer traffic and administration to a single service.
  - Accommodates all authorized Commercial Off-the-Shelf (COTS) file transfer products, leading to excellent architecture and interoperability.
  - Equips the Service Desk with "per file" transfer status monitoring in near real-time.
  - Stores aggregated relay logs, containing status, resource and security details useful for support efforts.
  - Provides a standard monthly status report with details about the relay usage for our partners' workload.
  - Enables partners to share in managing and monitoring various aspects of their file transfers.

- *Additional Benefits*
  - Allows partners to configure, update, and manage their own file transfer process(es).
  - Capable of sending 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 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).
  - Application. Although this service is COTS-centric, the service still applies scripting to enforce the security improvements, administrative savings, and each of the desirable benefits for our partners.
  - Management & standards, due to file transfer consolidation, centralization, and standardization.

NOTE: DISA CSD is actively looking for new solutions from vendors which are similar to SFG. DISA CSD recognizes SFG requires some changes to existing FTP scripts/parameters which on a large scale can be prohibitive for specific partners. If DISA CSD identifies and deploys a new solution, existing SFG partners will be moved to this solution.

3.2.3. Optional Features

Not Applicable

3.2.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

3.2.5. Service Rates

To find the rates associated with SFG Relay Service support, please contact your CSD CME team.

3.2.6. How to Order

SFG Relay Services are obtained by working with your CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

3.2.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to the CSD Terms & Conditions document.

3.3. Voice and Circuit Support

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

3.3.1. Description

DECC Columbus offers a variety of Voice and Circuit support services to local Columbus-area partners only. These 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 partners, and the exact terms and conditions are outlined with the description of each service.

3.3.2. Standard Features

- *Voice Services Telephone System Support*
  - DECC Columbus will provide a fully featured telephone line. This includes the capability for local calling in the commercial telephone network as well as long distance calling via Federal Telephone System (FTS), Direct Distance Dialing (DDD), International Direct Distance Dialing (IDDD), and Defense Switch Network (DSN). Standard features include: call forwarding, call holding, call transfer, name display, auto display, music on hold, and last number redial.
    - Maintain the telephone/cable system, to include problem troubleshooting and restoration.
    - Provide T-1 Trunking Services for Modem Pools, Fax Server Farms and others.
  - Basis for Reimbursement: partners will be billed a flat monthly rate per telephone line. This charge covers a fully featured telephone line with a standard single-line telephone with “stutter dial-tone” as the voice mail indicator and includes maintenance of the central office telephone switching system and software upgrades. The partner will be charged an additional fee for each multiple appearance of a directory number (MADN) occurrence and each electronic business set. The flat monthly rate will be charged for all active lines until DECC Columbus receives a work order notification to disconnect service. DECC Columbus will issue a detailed list of active lines upon the partner’s request.

3.3.3. Optional Features

- *Voice Services*
  - Telephone Usage Charges – In addition to the flat monthly rate per telephone line, the partner will be billed their portion of the Local Exchange Company telephone

bill, to include their local, toll, FTS, and DSN usage charges based on the Government Telephone Management Report. The invoice will include the Local Exchange Company's monthly service charge in addition to usage charges.

- The partner will be charged a flat monthly rate per T-1 installed. The partner will also incur additional fees for each Directory Number assigned and usage embedded in that T-1. Installation labor costs will be billed at the established rate.

- 1-800 Service – All of DISA DECC Columbus 800 numbers are inbound to the center. The partner selects what inbound Columbus they want it to ring in to. Charges are based on where the calling party is located, length of the call, and time of day. There are no cards assigned.
  - DECC Columbus will furnish 1-800 number service upon request of the partner. DECC Columbus ability to provision service may be limited by the contract vehicle in place.
  - Basis for Reimbursement: The partner will be charged a flat monthly administrative fee for each 1-800 service ordered plus monthly and recurring usage charges.
- Voice Mail Service
  - DECC Columbus will furnish voice mail services to include design, maintenance, installation/removal and administrative services.
  - Basis for Reimbursement: The partner will be charged a flat monthly rate per voice mailbox.
- Automatic Call Distribution (ACD) Service – The ACD system is a program feature residing in the MSL-100 switch operated by DECC Columbus. This feature allows inbound calls for individuals or contact centers to be distributed to agents logged into their system. Calls are routed by first in/first out priority. The calls are sent to an agent that has been in the longest wait state. Each agent has their own login for tracking data. The ACD functionality allows collection of call metric data such as number of inbound calls, duration of calls, and how long calls were held in queue before being answered.

  ACD tracking records can provide data to help assess agent performance. If multiple ACD groups are being used, they can be used in conjunction with our voice menu system where the caller can press "1" for this group or "2" for another group. Up to 10 groups can be connected by one master number.

  - DECC Columbus will furnish ACD service upon request of the partner. Services offered by DECC Columbus include: design, engineering, consultation, installation and maintenance. DECC Columbus will assist the partner in obtaining certified ACD equipment such as supervisory terminals and wallboards when requested.
  - Basis for Reimbursement

- The partner will be billed for material and actual labor costs incurred at the established hourly rate for engineering, design and consultation service including any additional license fees if Call Center Management Information System (CCMIS) services are requested. Hourly rates will also be applied while installing, modifying, relocating or disconnecting partners' ACD services.
- The partner will be charged a flat monthly rate per ACD agent to cover system administration and maintenance.

- Conference Bridge Service
  - DECC Columbus will furnish conference bridge services upon request of the partner. Bridge services are used by agencies located on the Defense Supply Center Columbus. Bridges are requested through local agency directorates. Bridges are normally only issued for 30 persons. Larger bridges may be available on an as-needed basis. Pass codes are issued for control. Bridges are issued on a temporary or permanent basis.
  - Basis for Reimbursement: The partner will be charged an administrative fee for each conference setup plus usage charges incurred by each conference participant.
- Integrated Services Digital Network (ISDN) Service – ISDN is the predecessor to Digital Subscriber Line (DSL). Both are data services available over regular telephone lines. ISDN Data rates tend to be limited to 128 Kbps. ISDN is a system of digital phone connections which is compatible with the existing (analog) telephone system. Our partners purchasing the ISDN service can use their phones to make conventional (analog, dialup) voice connections. In addition, ISDN partners can make high-speed digital data connections with other ISDN-capable telephone partners. There are two basic types of ISDN service: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Most individual and small business ISDN service consists of BRI Circuits. A BRI Circuit consists of two 64 kbps B channels and one 16 kbps D channel for a total of 144 kbps. With BRI service, two people can be using the B Channels for voice (conversations) simultaneously. Or a single 128Kbps Internet connection can be made using both B Channels. Or a 64Kbps Internet connection can be established using one B Channel, while the other B Channel is available for voice connections. ISDN is very flexible. It can be configured to connect to the Internet at 128Kbps and, if an incoming (voice) call arrives, dynamically release one B Channel (slowing the Internet connection to 64Kbps), freeing the other B Channel to handle the voice call.
  - DECC Columbus will furnish ISDN Basic BRI and PRI Services upon request of the partner. These services are used only for video teleconferencing.
  - Basis for Reimbursement

- For ISDN BRI, the partner will be charged a flat monthly rate for each directory number/line plus installation time and materials, as well as usage charges.
- For ISDN PRI, the partner will be billed a flat monthly rate for each PRI. The partner will also incur additional fees for each Directory Number assigned and usage embedded in that PRI. Installation labor costs will be billed at the established rate.

- Telephone Installations/Relocations/Disconnects
  - DECC Columbus will install, relocate and disconnect telephone/cable systems, upon request of the partner.
  - Basis for Reimbursement: The partner will be charged for actual labor, equipment, and material costs incurred while installing, re-locating or disconnecting partner telephone/cable systems. When applicable, labor rates will be reimbursed as standard or overtime hours. A standard hourly rate will be used for services provided from 0700 to 1600, Monday through Friday, excluding holidays. An overtime hourly rate will be applied for services provided outside the standard hours.
- Detailed Telephone Reports
  - DECC Columbus will furnish detailed "outbound" telephone call record reports upon request from the partner.
  - Basis for Reimbursement: The partner will be billed at the regular hourly labor rate required to run the requested report, for call records not more than six months old and a premium rate for reports that are more than six months old.
- Voice Menu Service
  - DECC Columbus will furnish voice menu/prompt maintenance service upon request of the partner. Services will include design, installation and testing of partner requested voice menu/prompt maintenance requirements.
  - Basis for Reimbursement: the partner will be billed for actual labor costs incurred at the established hourly rate for engineering, design and consultation of service.
- Direct Inward System Access (DISA) Lines – DISA lines are used by personnel who are temporarily teleworking or local agencies that require access to DSN and FTS long distance telephone service. These numbers are requested by local Directorates on an as-needed basis. Individual numbers and pass codes are issued as needed.
  - DECC Columbus will furnish DISA Lines upon the request of the partner.
  - Basis for Reimbursement: The partner will be charged a flat monthly rate, usage charges and installation time and materials.
- Voice/Data Engineering, Design and Consulting Service

        - DECC Columbus will furnish, at the partner's request, engineering, design and consulting services relating to all communication services.
        - Basis for Reimbursement: the partner will be billed for actual labor costs incurred at the established hourly rate of service.
    - Voice Circuits – T-1 (1.544MB) voice circuits are in support of partners located off of the Defense Supply Center Columbus (DSCC) base confines. The T-1s are via the local Exchange Carrier (AT&T) that provides service between the DISA Columbus Central Telephone Office and the offsite partner in support of a remote Private Branch Exchange (PBX) exchanges, Fax servers, or ISDN PRI VTC circuits.
    - Meridian Telephone Repair
        - DECC Columbus will furnish Meridian telephone repair service upon request of the partner. DECC Columbus' ability to provision service may be limited by the contract vehicle in place.
        - Basis for Reimbursement: the partner will be charged a flat rate for each repair service by telephone type.
- *Data Communications Support*
    - Circuit Extensions from Demarcation Point to partner – The DISA DECC Columbus Central Telephone Office is the demarcation Point of Presence (POP). Local Exchange Carriers (LECs) AT&T or Time-Warner deliver service to the demark location. In some cases the circuits may be required to be 'extended' to another part of the Columbus base (350+ acres). This may require the circuit to be extended via the DISA DECC Columbus underground cable plant (i.e. copper or fiber). In some cases, depending upon the distance, repeaters/modems may be required to support the partner's needs.
        - DECC Columbus will extend all circuits from POP in Building 23 to partner location(s).
        - Basis for Reimbursement: The partner will be charged a flat monthly rate for each circuit extended to cover the cost of equipment, maintenance and administrative services. Initial installation will be charged at the established hourly labor rate.
    - Circuit Engineering/Installation and Troubleshooting – A DECC Columbus representative will meet with the partner to discuss what is to be engineered, and to determine the best course of action and methodology to meet partner requirements. DISA will perform duties to include installation, testing, relocation, and troubleshooting of dedicated partner circuits. The circuit extension will utilize the DISA DECC Columbus underground cable plant using fiber or copper. In some cases, depending on distance restraints, repeaters or modems may be required to support the requirement. The Central Telephone Office and Outside Plant Installers will work with the partner to determine the most economical solution to meet partner needs.

        - DECC Columbus will install, relocate and troubleshoot dedicated partner circuits.
        - Basis for Reimbursement: The partner will be charged for actual labor, equipment, and material costs incurred.
    - Data Communications Installation/Relocations/Disconnects
        - DECC Columbus will install, relocate and disconnect data communication/cable systems, upon request of the partner. Communications relocations/disconnects will be worked through Work Orders via the DISA DECC GIG Global Infrastructure Service Management Center (GISMC) Service Desk. Authorized personnel from the partner's organization must open a ticket to have work completed.
        - Basis for Reimbursement: The partner will be charged for actual labor, equipment, and material costs incurred while installing, relocating or disconnecting partner Data Communication equipment. When applicable, labor rates will be reimbursed as standard or overtime hours.
- *LAN Support*
    - DECC Columbus will conduct capacity, performance and configuration management of existing LAN infrastructure to ensure that it delivers the level of service required to meet the partner's needs**.**
    - Basis for Reimbursement. The partner will be charged for actual labor, equipment, and material costs incurred.
- *Electronic Systems Support*
    - DECC Columbus Responsibilities. DECC Columbus will set up and operate portable public address system upon the partner's request.
    - Basis for Reimbursement: The partner will be billed for actual labor costs incurred at the established hourly rate of service.

3.3.4. Service Performance

For all Voice and Circuit support, in all four categories, the following Performance Objectives will apply:

- *Service Hours: Standard service hours are 0700 to 1600 hours, Monday through Friday, excluding holidays. When applicable, labor rates will be reimbursed as standard or overtime hours. An overtime hourly rate will be applied for services provided outside the standard hours.*
- *Telephone Outages: Upon receipt of a telephone outage notification by the partner during normal duty hours, 95% of those outages will be returned to service within eight (8) hours. The remaining 5% will be returned to service within 24 hours of notification. In cases where emergency services are affected, the response will be within one (1) hour.*

- *Installation/Relocation of Telephone Service: Upon receipt of the work order, the Provider will contact the partner and coordinate with other DISA organizations to plan and negotiate installation or relocation of telephone service. The Provider will make every effort to meet partner requested dates but due to already existing workload and the availability of materials, final dates will be negotiated as required.*

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA).

3.3.5. Service Rates

To find the fees associated with Voice and Circuit support, please contact your CSD CME team.

3.3.6. How to Order

Voice and Circuit services provided by CSD are obtained by working with your CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

3.3.7. Partner Responsibilities

For all Voice and Circuit support, in all four categories, the following partner responsibilities apply:

- *The partner will provide timely requests to the DECC Columbus Service Desk 614-692-1710 for installations, relocations, and disconnections of telephone and communication services.*
- *The partner will notify DECC Columbus of all personnel changes, including name, office symbol and telephone number changes. These changes may be submitted to DECC Columbus at 614- 692-1710.*
- *The partner will be required to reimburse DECC Columbus for all costs associated with missing leased equipment assigned to the partner.*
- *Excluded from coverage are hardware and/or software installed, modified and/or updated by the partner, client or technical persons other than DECC Columbus. If and when it is determined that said installation and/or modification was improper and is the cause and/or contributor to the problem, additional costs incurred for correction will be the sole responsibility of the partner. When this situation occurs, actual labor at the standard rate will apply, including any applicable material.*
- *For telework, the partner is required to obtain management approval to call forward their telephone line off center.*

To see the details behind partners', as well as other CSD, responsibilities, please refer to our CSD Terms & Conditions document.

4. SERVICES IN DEVELOPMENT

DISA CSD continues to research, design and deploy new service offerings which will bring higher levels of support to all 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. This section contains those service offerings which are in development and planned to be offered in full production in the near future.

4.1. DoD Enterprise E-Mail

*****NOTE: Currently being provisioned for selected Army users only*****

4.1.1. Description

DISA CSD will provide a DoD Enterprise Email Solution 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 CSD will be responsible for managing and operating the storage and server hardware, operating environment (OE), core E-mail applications, networking equipment and data center demilitarized zone (DMZ) security services necessary to create the connection between the Military Services, DoD Agencies, and DISA networks.

DISA CSD 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 CSD 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.

4.1.2. Standard Features

- *System Administration*
- *Security*
- *Data Communications*
- *Enterprise System Management (ESM) Software*
- *Level 2 Service Desk Support*
- *Storage*
- *Assured Computing/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 4GB (average) for thick client users and 500KB for web users*
- *Full Blackberry, Secure Mobile Environment-Portable Electronic Device (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 GISMC monitoring*
- *Full NetOps and CNDSP support*

4.1.3. Optional Features

- *Business Class Users*
  - SMTP to/from anywhere
  - OWA from anywhere
  - Outlook Anywhere (NIPRNET only)
  - Blackberry
  - Windows Mobile
  - 4GB average mailbox size
- *OWA Only Users*
  - OWA from anywhere
  - 500MB maximum mailbox size

4.1.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA).

4.1.5. Service Rates

To find the rates associated with DoD Enterprise E-Mail support, please contact your CSD CME team.

4.1.6. How to Order

DoD Enterprise E-mail services are obtained by working with your CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

4.1.7. Partner Responsibilities

The Military Service or Agency (user) being supported is responsible for the communications infrastructure necessary for leaving Post/Camp/Station/Base to connect users to the NIPRNet or SIPRNet. The user will continue to operate and manage their Active Directory (AD) forests and will grant DISA CSD access to these identity repositories to populate and synchronize E-mail contacts and accounts between the DOD Emergency Support Function (ESF) and the user AD forests (NIPR/SIPR).

Our partners must provide the tier 1 service desk that end users of the service must contact in the event of service incidents and outages. The tier 1 service desk provides the first line of support to end users of the service, and is the interface to DISA's DoD Enterprise Services service desk, known as the Global Infrastructure Services Management Center (GISMC). GISMC acts as the single POC for partner organization service desks for all DoD Email Service incidents. Basic requirements of the tier 1 service desk are:

- *Initiate all trouble tickets concerning the DoD Enterprise Email Service*
- *Provide triage and rule out local system and/or network issues and best effort to resolve incident to close the trouble ticket*
- *As necessary escalate the ticket to DISA CSD GISMC Tier II support for resolution*
- *Interact with partners' end users for all enterprise email issues*
- *Interact with GISMC on behalf of end user community.*

To see the details behind partners', as well as other CSD, responsibilities, please refer to the CSD Terms & Conditions document.

4.2. Enterprise SharePoint Service

4.2.1. Description

Offered initially on the NIPRNet, Enterprise SharePoint Service (ESPS) is a dedicated SharePoint Hosting Service providing Combatant Commands, Military Services, and DoD Agencies (CC/S/A) 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 (MS) SharePoint (SP) 2010 platform, this service will provide organizations the ability to create and manage mission, community, organization, and user focused sites for collaboration. Our partners will be provided the ability to customize and manage their site collections and content as well as apportion their allocated storage among their site collections without the additional burden of managing the infrastructure. DISA CSD will manage the multi-tenant environment and chair the Configuration Control and Governance Boards.

ESPS benefits from the economies of scale possible from common Infrastructure as a Service (IaaS) capabilities provided by the DECC. Server hosting, network components, and out-of-band (OOB) system management capabilities may be shared but with accommodation for separate logical data storage, server OEs, applications, and network enclaves to provide a clearly defined boundary isolating risk between partners.

This service offering will be flexible to each of our partner's needs, as it utilizes a per-user pricing model and can be a shared service or dedicated hosting, based upon the partner's size and customization needs.

4.2.2. Standard Features

- *Users can log in from anywhere in the world*
- *99.9% Availability*
- *Tier II Service Desk Support*
- *Authentication – The Enterprise Application and Services Forest (EASF) will be used to authenticate users; users must authenticate directly with the SP platform with a transport layer security (TLS) session and their common access card (CAC).*
- *Storage – Each partner will be allocated storage based on the number of subscribers in their user base, and it is important to note that SP is intended to be a collaboration platform rather than primary storage. A separate service offering for cloud-based storage will be developed and will be much more economical than using SP for primary storage.*
    - There is an offsite backup for COOP; however, both sites will not be providing service at the same time
    - Selective restore at the file/object granularity will be provided up to 30 days and 10% of our partner's capacity

  - Databases are backed up every eight (8) hours with more frequent incremental backups

- *Content and Records Management*
  - ESPS content is considered to be unmanaged (DoD 5015.2). For managed content, a separate enterprise service for Records Management will be developed that manages content throughout its lifecycle. ESPS will be integrated with the Enterprise Records Management (ERM) service offering.

- *Development and Staging*
  - DISA CSD will provide guidance and a test bed; our partner is responsible for SP content management, application development, and migration

- *Configuration Management (CM)*
  - Our partner will be afforded an opportunity to request changes to the base configuration. DISA CSD will chair a Configuration Control Board (CCB) to govern such changes.

- *Time to Implement*
  - Approximately 60 days from when funding and approvals are received

- *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*
- *External user access sites which may be isolated from internal organizational sites*
- *Ability to search SharePoint site content across the service or within sub-sites*
- *E-mail alerts when documents and information have been changed or added to a site*
- *Internet accessible private and public content publishing*
- *Scalability to thousands of sites within an organization, so that managers can delegate site creation to others*
- *Dedicated servers, networks, and physical space in DECCs*

4.2.3. Optional Features

- *Additional storage to accommodate growth*
- *Granular content backup/restoration capability for site and item level recovery*
- *Enhanced enterprise SharePoint administration tools beyond those available within SharePoint out-of-the-box*
- *Site-to-site COOP/Disaster Recovery capability*
- *WAN acceleration and content delivery service to improve edge user experience and system response times*

- *Add on applications such as MS Project and CRM*

4.2.4. Service Performance

Service performance is measured, monitored, and reported as defined in the DISA CSD Service Level Agreement (SLA). For additional information, please refer to the CSD Service Performance Levels.

4.2.5. Service Rates

In Development

4.2.6. How to Order

ESPS services provided by CSD are obtained by working with a CSD CME team to develop a Service Request Form (SRF) that will identify the specifics of your requirement.

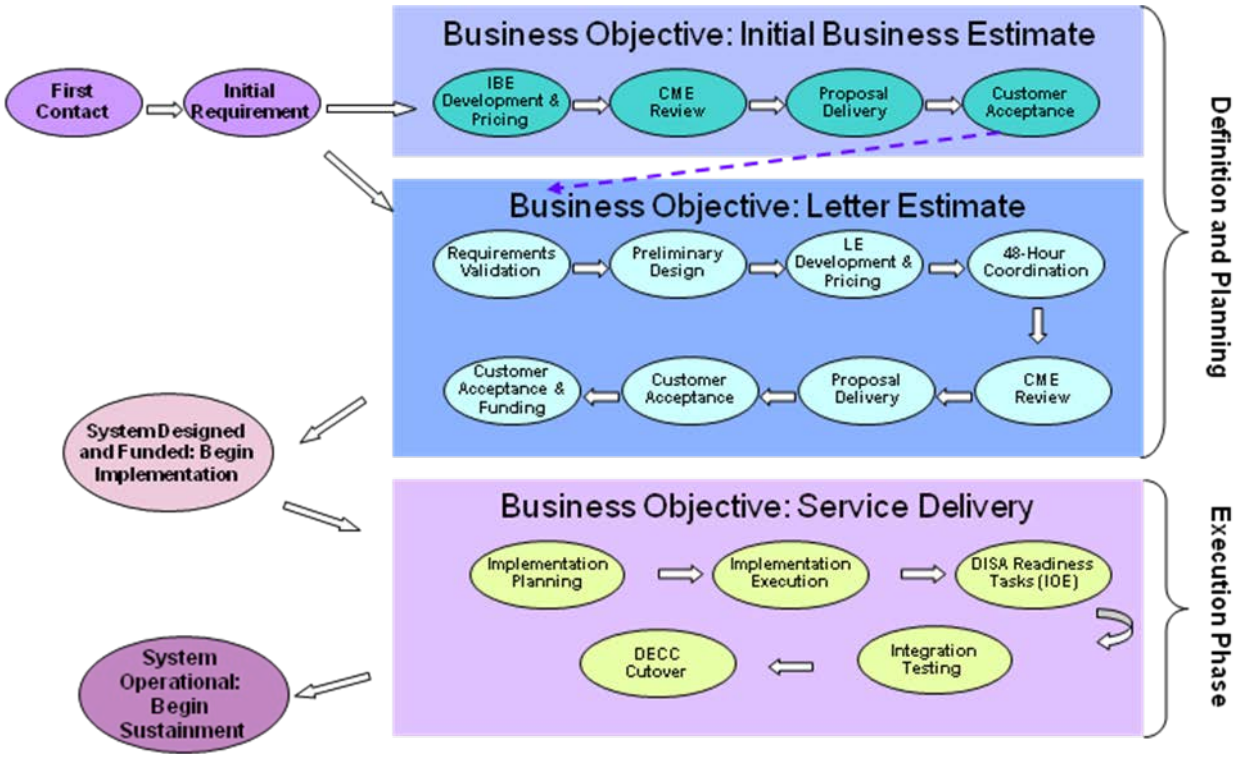
To obtain contact information for your CME team or the SLM Hotline, please refer to the Points of Contact section.

4.2.7. Partner Responsibilities

To see the details behind partners', as well as other CSD, responsibilities, please refer to the CSD Terms & Conditions document.

5. ADDITIONAL INFORMATION

5.1. DISA CSD Business Model



5.2. DISA CSD Inherited IA Controls

DISA CSD has documented the following Inherited Information Assurance (IA) Controls in accordance with (IAW) DIACAP:

Control	Control Name	Description	Supporting Rational
COPS-1	Power Supply	Electrical power is restored to key IT assets by manually activated power generators upon loss of electrical power from the primary source.	This control is satisfied by the site and a system cannot satisfy the requirement.
COPS-2	Power Supply	Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators.	This control is satisfied by the site and a system cannot satisfy the requirement.
COPS-3	Power Supply	Electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source.	This control is satisfied by the site and a system cannot satisfy the requirement.
DCDS-1	Dedicated IA Services	Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.	This control is always either compliant or non-compliant based upon the enterprise.

Control	Control Name	Description	Supporting Rational
DCSP-1	Security Support Structure Partitioning	The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.	The site is responsible for ensuring isolation is maintained for systems which are installed at the site. Individual systems cannot accomplish this IAC.
EBBD-1	Boundary Defense	Boundary defense mechanisms, to include firewalls and network Intrusion Detection Systems (IDS), are deployed at the enclave boundary to the WAN. Internet access is permitted from a DMZ that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means. All Internet access points are under the management and control of the enclave.	The enterprise is responsible for the boundary defense mechanisms and IDS system deployment. This cannot be accomplished by a system within the enterprise.
EBBD-2	Boundary Defense	Boundary defense mechanisms, to include firewalls and network IDS, are deployed at the enclave boundary to the WAN and at layered or internal enclave boundaries, or at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.	The enterprise is responsible for the boundary defense mechanisms and IDS system deployment. This cannot be accomplished by a system within the enterprise.

Control	Control Name	Description	Supporting Rational
EBBD-3	Boundary Defense	Boundary defense mechanisms, to include firewalls and network IDS, are deployed at the enclave boundary to the WAN and at layered or internal enclave boundaries and key points in the network as required. All Internet access is prohibited.	The enterprise is responsible for the boundary defense mechanisms and IDS system deployment. This cannot be accomplished by a system within the enterprise.
EBPW-1	Public WAN Connection	Connections between DoD enclaves and the Internet or other public or commercial WANs require a DMZ.	Connections of enclaves and the internet or other public or commercial WANs is the responsibility of the enterprise. This control cannot be accomplished by a system within the enterprise.
EBVC-1	VPN Controls	All VPN traffic is visible to network IDS.	The enterprise is responsible for performing IDS monitoring and therefore must be capable of monitoring VPN as well as all other traffic.
ECIM-1	Instant Messaging (IM)	IM traffic to and from IM clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service IM traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.	Blocking of the inbound and outbound traffic is the responsibility of the enterprise and this control cannot be accomplished by a system within the enterprise.

Control	Control Name	Description	Supporting Rational
ECND-1	Network Device Controls	An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files; and a structured process for implementation of directed solutions (e.g., IAVA).	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
ECND-2	Network Device Controls	An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files; and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
PECF-1	Access to Computing Facilities	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.	Ensuring only authorized personnel are granted access to a site is the responsibility of the site. A system cannot satisfy this requirement.

Control	Control Name	Description	Supporting Rational
PECF-2	Access to Computing Facilities	Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.	Ensuring only authorized personnel are granted access to a site is the responsibility of the site. A system cannot satisfy this requirement.
PEEL-1	Emergency Lighting	An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEEL-2	Emergency Lighting	An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEFD-1	Fire Detection	Battery-operated or electric stand-alone smoke detectors are installed in the facility.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEFD-2	Fire Detection	A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEFI-1	Fire Inspection	Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEFS-1	Fire Suppression	Handheld fire extinguishers or fixed fire hoses are available should an alarm be sounded or a fire be detected.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEFS-2	Fire Suppression	A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke, or particles.	This control is satisfied by the site and a system cannot satisfy the requirement.

Control	Control Name	Description	Supporting Rational
PEHC-1	Humidity Controls	Humidity controls are installed that provide an alarm of fluctuations potentially harmful to personnel or equipment operation; adjustments to humidifier/de-humidifier systems may be made manually.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEHC-2	Humidity Controls	Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEMS-1	Master Power Switch	A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEPF-1	Physical Protection of Facilities	Every physical access point to facilities housing workstations that process or display sensitive or unclassified information that has not been cleared for release is controlled during working hours and guarded/locked during non-work hours.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEPF-2	Physical Protection of Facilities	Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X 7. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics). A visitor log is maintained.	This control is satisfied by the site and a system cannot satisfy the requirement.

Control	Control Name	Description	Supporting Rational
PEPS-1	Physical Security Testing	A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.	This control is satisfied by the site and a system cannot satisfy the requirement.
PESP-1	Workplace Security Procedures	Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.	This control is satisfied by the site and a system cannot satisfy the requirement.
PETC-1	Temperature Controls	Temperature controls are installed that provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually.	This control is satisfied by the site and a system cannot satisfy the requirement.
PETC-2	Temperature Controls	Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.	This control is satisfied by the site and a system cannot satisfy the requirement.
PETN-1	Environmental Control Training	Employees receive initial and periodic training in the operation of environmental controls.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEVC-1	Visitor Control to Computing Facilities	Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.	This control is satisfied by the site and a system cannot satisfy the requirement.
PEVR-1	Voltage Regulators	Automatic voltage control is implemented for key IT assets.	This control is satisfied by the site and a system cannot satisfy the requirement.

5.3. Customer Service

DISA CSD provides focused customer management services. The Customer Management Division is structured by the major DoD partner, Service or Agency. There are currently seven branches (CME branches) established:

- *DFAS/DLA/BTA/USTRANSCOM*
- *ARMY*
- *MHS*
- *DoD/Joint Staff/COCOM*
- *AIR FORCE*
- *NAVY/MARINE CORPS*
- *DISA*

Each CME Branch is lead by a government official with overall responsibility for their Customer Management Team. Each Customer Management Team consists of, at a minimum, one or more of the following members:

- *Customer Team Lead*
- *Customer Account Representative (CAR)*
- *Technical Representative/Engineer*

The Customer Management Team will be responsible for all business events related to our partner's experience. During the typical project life cycle, this may include fielding initial partner requirements, developing associated proposals with DISA CSD service description and pricing, planning and coordination of implementation events (scheduling, acquisition, logistics, testing, etc.) and operational transition into a production mode.

The establishment of the Customer Management Team(s) will provide our partners one place to obtain answers on business issues from initiation to production status. This same group will perform a myriad of functions including: SLM; financial management (i.e. funding coordination, billing and invoicing); inventory management; service outreach; annual budgeting and planning; regular review and analysis of workload efficiency; and technical refresh of equipment.

Customer Service features dedicated, multi-skilled teams for each major DoD partner, Service or Agency. Those teams consist of information technology technicians, project managers, CARs, and systems and software engineers. Included in the responsibilities of this division are:

- *Creation and maintenance of Service Level Agreements (SLAs)*
- *Preparation of engineering designs and business proposals for new partner workload*
- *Project management of new workload implementations*

- *Handling all issues and questions identified by our partners*
- *Joining with our partners to develop strategies that achieve cost savings and efficiencies*

Customer Service has a standard approach to addressing partner inquiries and maintaining partner relationships. As unique requirements exist, Customer Service representatives can discuss options for dedicated support that a partner may require to successfully define and deploy project workload.

5.4. DISA CSD Partner Portal

The CSD Partner Portal is located at https://ciws.csd.disa.mil/cp/default.aspx. If you do not yet have a Partner Portal account, please contact your Customer Account Representative (CAR) for registration instructions.

DISA CSD Service Level Management (SLM) has developed the Partner Portal web site a valuable repository of information where registered users can download documents such as our Service Catalog, Terms and Conditions and Rate Schedule, as well as view their Service Level Agreements (SLAs) and Planning Estimates (PEs).

- *Located as an extension of the Consolidated Internal Web Site (CIWS), the Partner Portal is managed solely by CSD SLM personnel. There is no one between the partners and CSD.*
- *Provides web access to your SLAs with CSD*
  - All our partners that have one or more SLAs with DISA will have view access to their SLAs.
  - All CSD personnel have view access to SLAs to assist in seamless end-to-end partner support
  - All of our current SLAs are arranged by Service/Agency and linked to the Service Catalog and the Terms and Conditions (T&C) document so that the full range of information about our service offerings is immediately available.
- *Access to DISA CSD templates*
  - SLA template and guidance – the standardized framework and guidance necessary to build all CSD SLAs
  - Service Request Form (SRF) templates
  - Letter Estimate (LE) template
  - Initial Business Estimate (IBE) template
  - Solution Document template
- *Home to the single official CSD Service Catalog and T&C*
- *Links to Information Assurance (IA) documents, such as:*
  - IA Guidance
  - DoD IA Certification and Accreditation Process (DIACAP) Guidance
  - Mission Assurance Category (MAC)/Confidentiality Level IA Controls

- *Frequently Asked Questions (FAQs) including common questions that come to CARs, our Service Desks and from other sources of partner interaction.*
- *Access to the portals for the Rapid Access Computing Environment (RACE), Global Content Delivery Service (GCDS), and Forge.mil. Access to the DISA Worldwide Financial Network (DWFN), where electronic partner invoices reside.*
- *Access to Interactive Customer Evaluation (ICE) comment cards and partner satisfaction surveys regarding your satisfaction with CSD's services and performance.*
- *Repository for DISA CSD Policies, Electronic Business Systems (EBS) Metrics, and Capacity Management Reports*
- *DISA CSD contact information*
- *Other links, notes, and announcements.*

5.5. Host-Based Security System

For a more detailed service offering description, please visit www.disa.mil/hbss.

The Host-Based Security System (HBSS) baseline is a flexible, commercial off-the-shelf (COTS) based application. The system can detect and counter cyber threats to a DoD enterprise in real time. Under the sponsorship of the Enterprise-wide Information Assurance (IA) and Computer Network Defense Solutions Steering Group (ESSG), the HBSS solution will be attached to each host (server, desktop, and laptop) in the DoD.

The system will be managed by local administrators and configured to block known bad traffic using an Intrusion Prevention System (IPS) and host firewall. DISA's Program Executive Office for Mission Assurance (PEO-MA) is providing the program management and supporting the deployment of this solution.

The scope of the HBSS deployment is worldwide. This vast effort requires a large support infrastructure to be in place. The DISA PEO-MA has instituted support services that will enable the comprehensive implementation of HBSS to all the combatant commands, services, agencies and field activities.

The many capabilities and services associated with HBSS are:

- *ePolicy Orchestrator (ePO) management suite is a central security manager that enables the installation, management, and configuration of the HBSS components.*
    - Common Management Agent (CMA) provides local management of all HBSS products collocated on the host. CMA runs silently in the background to gather information and events from managed systems. It sends collected data to the ePO server and manages modules and software updates of other HBSS products on the host system; furthermore, it enforces policies on the host machines.
- *Host Intrusion Prevention System (HIPS) plug-in module enforces security policy. It adds a robust layer of protection to the CMA end-point asset that includes known and unknown buffer overflow exploit protection, prevention of malicious code installation/execution, and identification of activities that deviate from DoD or organizational policy.*
- *Asset Baseline Monitoring (ABM) (in support of the Information Condition [INFOCON]) plug-in module generates snapshots of asset configurations to facilitate detection of changes made to authorized baselines.*
- *Device Control Module (DCM) prevents unauthorized USB and flash media devices from being plugged into End-Point systems. It also allows restrictions and/or exceptions based on specific hardware IDs, vendor IDs and serial numbers.*
- *Policy Auditor (PA) scans remote computers to determine compliance with defined policies. Identifies host vulnerabilities on the network.*

- *Rogue System Detection (RSD) is used to detect and react to unmanaged (or rogue) systems present on the network.*

5.6. Operating Environment Sizing

The rate-based server billing methodology workload unit is the operating environment (OE). An OE is defined as an instance of operating system (OS) software. An OE can be a single physical server or a logical server partition. The size of the OE is determined by the number of populated sockets being used. A socket is defined as a connector linking the motherboard to the CPU(s). (The number of "cores" on the chip is not part of the equation.)

The rate-based Basic category has been consolidated into levels, but is still size dependent. Hardware Service continues to be size and platform dependent. The Database Software (Oracle DBMS only) service is OE size dependent, but not platform dependent. The remaining labor-based rate (such as Application Support, Database Administration, and 24x7 Services) are size and platform agnostic.

- *Basic (any platform OE)*
  - Level 1- Reserved for future use
  - Level 2 – Virtualized OE less than one socket
  - Level 3 – One (1) to two (2) sockets per OE
  - Level 4 – greater than two (2) sockets, up to and including four (4) sockets per OE
  - Level 5 – greater than four (4) sockets, up to and including eight (8) sockets per OE
  - Level 6 – greater than eight (8) sockets per OE
- *Hardware Services*
  - OEs running x86 chipset hardware (generally Windows and Linux OSs)
    - Level 1 – Reserved for future use
    - Level 2 – Virtualized OE less than one (1) socket
    - Level 3 – one (1) to two (2) sockets per OE
    - Level 4 – greater than two (2) sockets, up to and including four (4) sockets per OE
    - Level 5 – greater than four (4) sockets per OE
  - OEs running Non-x86 chipset hardware (generally UNIX OSs)
    - Level 1 – Reserved for future use
    - Level 2 – Virtualized OE less than one (1) socket

- Level 3 – One (1) to two (2) sockets per OE
- Level 4 – greater than two (2) sockets, up to and including four (4) sockets per OE
- Level 5 – greater than four (4) sockets, up to and including eight (8) sockets per OE
- Level 6 – greater than eight (8) sockets, up to and including 20 sockets per OE

NOTE: OEs over 20 sockets are priced c-goal, outside of the rates for Hardware Service, but all other services are still priced within the rate-based pricing environment.

- *Database Software (any platform or size OE)*
  - Level 1 – Reserved for future use
  - Level 2 – Virtualized OE less than one (1) socket
  - Level 3 –One (1) to two (2) sockets per OE
  - Level 4 – greater than two (2) sockets, but less than or equal to four (4) sockets per OE
  - Level 5 – greater than four (4) sockets, but less than or equal to eight (8) sockets per OE
  - Level 6 – greater than eight (8) sockets, but less than or equal to 20 sockets per OE

5.7. Service Desk

DISA CSD uses Total Contact Management and industry best practices as a systemic approach to managing the client relationship, whereby ownership and accountability in the organization are keys to successful partner care and a measurement of service support. It has proven to be a simplified, predictable, professional, high-quality service interface for post-deployment support for partner/DISA CSD agreed upon services outlined in the SLA. This approach addresses services which include, but are not limited to, a support environment through an integrated common set of tools, processes, workflows, and human resource management based on proven best practices.

The Service Desk is partner-focused, with a trained support staff ready to address a partner's request. As soon as the staff responds to a call, they "own" the incident or problem and are responsible for obtaining information from the partner in an organized and professional manner. This process includes incident and problem management with continual follow up until the issue or question is resolved to the partner's satisfaction.

Key objectives include:

- *Ensuring that CSD provides consistent, knowledgeable interactions with partners*
- *Integrating partner focus into everyday operations*
- *Providing high-quality, predictable, and professional partner interfaces*
- *Partnering with and supporting a specific partner, with responsibility and accountability to that partner*
- *Shortening the response timeline for the resolution of partner problems*
- *Ensuring a consistent point of contact for the diverse concerns of each partner*

The Service Desk manager has oversight responsibility for development, continuous improvement, and uniform implementation of Service Desk support standards and processes.

Service Desk managers and operations staff are responsible for accomplishing all assigned activities, tasks, and functions in accordance with all work instructions.

The management and operations staff is also responsible for notifying the Service Desk manager if any information is incorrect or needs improvement.

The Service Desk managers are responsible for assigning accountability for each contact received. Service Desk representatives receive contacts through multiple media such as phone, message queue, and email. For those calls that are not resolved upon first contact, the assigned Service Desk manager is responsible for pursuing resolution in accordance with applicable SLA and operating procedures.

Follow-up notification to the partner is the responsibility of the Service Desk manager, in accordance with the established SLA. When an incident occurs, it is the responsibility of the applicable Service Desk to resolve the incident.

Our partner support provides efficient interfaces between traditional partner service providers, technical support elements, operations, and external support organizations (such as vendors). These interfaces are supported via common standards, integrated common tool suites, and common enterprise procedures as well as the removal of traditional barriers, both physical and procedural. Our successful Service Desk relies on the knowledge elements that pertain to the partner's post-deployment support.

These services are defined as follows:

- *Mid-Level Expertise*
- *Senior-Level Expertise*
- *Technical Support*
- *External Support*

The Service Desk utilizes the following Processes and Sub-processes:

- *Communicating with partners*
  - Responding to Initial Contacts
  - Conduct Ongoing Communications
  - Completing communications
- *Assigning Accountability*
- *Finding Solutions*
- *Resolving Trouble Management Actions Requests*
- *Providing Tracking*

Receiving System-Generated Information

System-generated information consists of system alerts or messages that are internally generated by indirect contacts. A message/alert notifies the Service Desk of a system event or condition that may provide information affecting one or more open incidents. These events may be manually monitored, or they may have automated interfaces that generate a notification or even initiate a ticket in the tracking system.

Examples may include:

- *If significant, the system alert/messages initiate a notification*

- *The message/alert has the characteristics of either a first contact or a follow-on contact*
- *Dependent on the initial root cause analysis, the appropriate action will be taken*

Overview

DISA CSD is dedicated to monitoring the success of support delivery on all promised service levels and ensuring partner satisfaction. DISA CSD wants partners to know that someone understands the business impact of their issues, empathizes with their situations, and will "stay with them" until the issue is resolved.

DISA CSD is in a constant state of improvement with leading edge operational philosophy, technical procedures and tools for maintaining partner relationships. The Service Desk supports a strong, partner-focused environment and highly responsive post-deployment support services. Common standards, procedures, and centralized enterprise tools for all operating locations ensure partners receive the same predictable high-quality services regardless of processing location. Success in meeting these responsibilities must be addressed from both the internal operations perspective and the external partner perspective.

Ticket Priorities

- *Five (5): Indicates maintenance or a scheduled action.*
- *Four (4): Results in user/operator inconvenience or annoyance, but does not affect a required operational or mission essential capability; results in inconvenience or annoyance for development or support personnel, but does not prevent the accomplishment of those responsibilities.*
- *Three (3): Adversely affects the accomplishment of an operational or mission essential capability, but a work-around solution is known; adversely affects technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known.*
- *Two (2): Adversely affects the accomplishment of an operational or mission essential capability and no work-around solution is known; adversely affects technical, cost, or schedule risks to the project or life-cycle support of the system and no work-around solution is known. Based on DISA Policy criteria of Action Type and length of outage, this action request could be reportable to the GNC.*
- *One (1): Prevents the accomplishment of an operational or mission-essential capability; jeopardizes safety, security, or other requirement designated critical. Based on DISA Policy criteria of Action Type and length of outage, this action request could be reportable to the GNC.*

Service Desk Levels of Support

- *Level I*
    - Optional service (additional cost to partner)
    - Calls received: from end user to Service Desk

- First call is to DISA CSD for resolution
- Open tickets

- *Level II*
  - Basic service (included within the rates)
    - Tier I CSP
    - Security
    - Core OS & ESM Software maintenance
    - Tier II System Administration (SA) (if managing the servers)
      - Mon-Fri (0800-1600)
      - 2 hour call back for emergencies
      - 1 x per month, scheduled maintenance window
  - Extended to every workload we manage
  - Calls received from component's Service Desk
  - Service Desk to Service Desk (e.g. LI-LII, LII-LII, LIII-LII)
  - Partners' end users call component's Service Desk

- *Level III*
  - Optional service (additional cost to partner)
  - Calls received from Vendor/subject matter expert (SME) Service Desk to Service Desk
  - Issues elevated to 3rd party (i.e. BOC, Oracle, McAfee, SUN, Microsoft)
  - Possess intimate knowledge of a given business, such as:
    - Logistics
    - Accounting and finance
    - Security
    - Health Care
    - Software package or other subject matter

- Vendor support

Service Desk Skill Set Tiers

- *Tier I*
  - Basic service (included within the rates)
  - Customer Service Professional (CSP) Support
  - Open tickets
  - Collects partner contact and incident information
  - Provides ticket number
  - 5-10 minute First Call Resolution (FCR)
  - Unable to resolve, assigns to Tier II
  - Password resets
  - Answers phones/emails 24x7
  - Redirects misrouted calls
  - Ensures consistent ticket updates
  - Notifies Service Desk Lead on critical/high visibility incidents
  - Closes fixed tickets
  - Proactive asset infrastructure monitoring
- *Tier II*
  - Optional service (additional cost to partner)
  - Application Support
  - Specific application support
    - Load application release/patches
    - Application management and modification
  - Tech Support
    - DBA

        - SA
            - Operating Environment

- *Tier III*
    - Optional service – not routine (additional cost to partner)
    - External Support
    - Vendor
    - Developer for specific product/service

5.8. Enterprise System Management Software

Enterprise System Management (ESM) software are the tools DISA CSD uses to monitor the health and well-being of our partners' information systems and data and to manage problems when (and sometimes before) they occur. These tools alert DISA CSD when conditions are favorable for problems to manifest themselves, so DISA CSD can get the appropriate technicians on the scene to resolve any potential problems before they occur

APPENDIX A – ACRONYMS

The following acronyms are referenced throughout this Service Catalog.

Acronym	Definition
ACD	Automatic Call Distribution
AD	Active Directory
AIS	Automated Information System
ASC	Application System Code
ATAAPS	Automated Time Attendance and Production System
ATO	Authority to Operate
BAC	Business Availability Center
BAN	Billing Account Number
BCP	Business Continuity Plan
BMC	Business Management Center
BOM	Bill of Materials
BPM	Business Process Monitor
BRI	Basic Rate Interface
C/A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CAM	Customer Account Manager
CAPS	Collaboration and Process System
CAR	Customer Account Representative
CCMS	Call Center Management Information System
CDA	Central Design Activity
CERT	Computer Emergency Response Team
CIC	Customer Identification Code
CIS	Centralized Invoice System
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CME	Customer Management Executive

Acronym	Definition
COIN	Community of Interest Network
CONUS	Continental United States
COOP	Continuity of Operations
CPU	Central Processing Unit
CSD	Computing Services Directorate
CSP	Customer Service Professional
DAA	Designated Approving Authority
DASD	Direct Access Storage Device
DBA	Database Administrator
DBSMC	Defense Business Systems Management Committee
DBT	Defense Business Transformation
DDD	Direct Distance Dialing
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DISA	Direct Inward System Access
DISN	Defense Information Systems Network
DIACAP	DoD Information Assurance Certification and Accreditation Process
DLA	Defense Logistics Agency
DMS	Defense Messaging Services
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoD	Department of Defense
DODAAC	DoD Activity Address Code
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DRA	DAA Risk Acceptance
DSCC	Defense Supply Center Columbus
DSD	Data System Designator

Acronym	Definition
DSL	Digital Subscriber Line
DSN	Defense Switch Network
EASF	Enterprise Application and Services Forest
EBS	Electronic Business Systems
ECA	Enterprise Connection Approval
eMASS	Enterprise Mission Assurance Support Service
ESSG	Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group
ESPS	Enterprise SharePoint Service
FFS	Fee-for-Service
FIPS	Federal Information Processing Standards
FMLO	Financial Management Liaison Office
FORCECON	Force Condition
FTS	Federal Telephone System
FW	Firewall
FY	Fiscal Year
GEX	Global Exchange
GCCS	Global Command and Control Services
GCDS	GIG Content Delivery Service
GCSS	Global Combat Support Services
GIG	Global Information Grid
GISMC	Global Infrastructure Service Management Center
GNC	Global NetOps Center
GUI	Graphic User Interface
GS	Combat Support Directorate
HP	Hewlett-Packard
IA	Information Assurance
IaaS	Infrastructure as a Service
IAC	Invoice Account Code
IAM	Information Assurance Manager

Acronym	Definition
IAO	Information Assurance Officer
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IBE	Initial Business Estimate
ICE	Interactive Customer Evaluation
IECA	Interim Enterprise Connection Approval
IIS	Internet Information Services
IM	Instant Messaging
IDDD	International Direct Distance Dialing
IS	Information System
INFOCON	Information Condition
INFOSEC	Information Security
I/O	Input/Output
IOC	Initial Operational Capability
IOE	Initial Operating Environment
IP	Internet Protocol
IRB	Investment Review Board
ISDN	Integrated Services Digital Network
IT	Information Technology
ITSCM	Information Technology Service Continuity Management
KPI	Key Performance Indicators
LAN	Local Area Network
LPAR	Logical Partition
LE	Letter Estimate
MAC	Mission Assurance Category
MADN	Multiple Appearance of a Directory Number
MBL	Measured Business Line
MIAG	Mandatory Information Assurance Guidance
MIAP	Mainframe Internet Access Portal

Acronym	Definition
MIPR	Military Interdepartmental Purchase Requests
MOSS	Microsoft Office SharePoint Server
MRC	Monthly Recurring Charge
NDAA	National Defense Authorization Act
NIPRNet	Non-Classified (but Sensitive) Internet Protocol Routing Network
OCONUS	Outside of the Continental United States
OE	Operating Environment
OEM	Oracle Enterprise Manager
OPM	Office of Personnel Management
OPX	Off Premise Exchange
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
PBX	Private Branch Exchange
PE	Planning Estimate
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Point of Presence
PPS	Proposal Pricing System
PPSM	Ports, Protocols, and Services Management
PRI	Primary Rate Interface
RACE	Rapid Access Computing Environment
RDT&E	Research, Development, Test & Evaluation

Acronym	Definition
RPO	Recovery Point Objective
RSD	Rogue System Detection
RTO	Recovery Time Objective
RUM	Real User Management
SA	System Administrator
SCP	System Compliance Profiler
SF 1080	Standard Form 1080
SFUG	Security Features User's Guide
SIPRNet	Secret Internet Protocol Routing Network
SLA	Service Level Agreement
SMC	Systems Management Center
SME	Subject Matter Expert
SME-PED	Secure Mobile Environment-Portable Electronic Device
SOE	Standard Operating Environment
SRF	Service Request Form
SSL	Secure Socket Layer
SSO	Single Sign On
STIG	Security Technical Implementation Guide
SyNAPS	System Network Availability Performance Service
T&C	Terms and Conditions
TCP	Transmission Control Protocol
TDY	Temporary Duty
TMS	Trouble Management System
UIC	Unit Identification Code
UPS	Uninterruptible Power Supply
VMS	Vulnerability Management System
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WCF	Working Capital Funds

APPENDIX B – GLOSSARY

Term	Description
Accreditation	Formal declaration by a Designated Approving Authority (DAA) that an Information System (IS) is given approval to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (DoD 8510-1.M, Jul 31 2000)
Amendment	Additive terms and provisions to the SLA.
Batch Throughput	Completion rate and delivery by specified time during the "Batch Window" as specified in the SLA.
Bill	A Standard Form 1080, issued by the Defense Finance and Accounting Service (DFAS), which constitutes an official request to pay for services delivered. Bills present only summary data on charges to the partner. Detailed charge information supporting the bill can be found on the invoice available via the DISA Centralized Invoice System (CIS).
Business Continuity Plan (BCP)	Advance arrangements and procedures which enable an organization to respond to an event in such a manner that the critical business functions continue with minimal interruption or essential change.
Defense Business Transformation (DBT)	DoD program to transform business operations to achieve improved Warfighter support while enabling financial accountability across the DoD. DBT will implement enterprise level business capabilities that will accelerate department-wide improvements in business processes and information systems.
Capital Items/Expenses	Computer equipment and software that must be purchased using WCF acquisition (i.e., capital investment) dollars.
Certification	Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. (DoD 8510-1, Jul 31 2000)

Term	Description
Charges	Amount the partner is required to pay for the services delivered.
Confidentiality Level	Determined by whether the system processes classified, sensitive, or public information.
Customer Account Representative (CAR)	A representative of DISA CSD who serves as the primary point of contact to the partner for DISA CSD services. The CAR is responsible for assuring the partner is satisfied with DISA CSD services.
DASD Services	Provide the partner with daily/weekly backup of partner data (daily incremental, daily full volume dumps, and/or data base logs).
Data Retrieval Services	Partner data retrieval from archive tape (square or round) either on-site, off-site local, or off-site backup site.
Depreciation	That portion of the cost for a capital investment item that applies to an accounting period. Federal information processing resources (CPUs, DASD, Server HW, etc.) are depreciated monthly over the useful life of an asset using the "straight-line depreciation" method. As an example, an asset with a three (3) year useful life (36 months) with a capital cost of $X, would be expensed monthly at $X/36 = monthly depreciation expense. Depreciation is part of the Fee-for-Service (FFS) rate when FFS rates apply to a specified DISA CSD service. Otherwise, it is part of the charge for a particular non-rate based reimbursable service.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. (DoD 8510-1.M, Jul 31 2000)
Disaster Recovery Plan	Provides the procedures for restoring partners' information system requirements in the event of a disaster.
Domain Name Service (DNS)	An Internet service that translates domain names into IP addresses.

Term	Description
Downtime	Time when the system or network is not available to the user. The downtime may be scheduled, as for routine maintenance, or unscheduled.
Exception to Normal Processing	Temporary requirements that cannot be accommodated within agreed-to levels of services or customary procedures.
Final Operational Capability (FOC)	A system is declared FOC if it runs continuously without any issues for 30 days after IOC declaration.
GIG Content Delivery Service (GCDS)	Provides a DISN enterprise level service to accelerate delivery and improve reliability of web applications.
In-Cycle Changes	Refers to permanent changes to workload estimates or technical requirements occurring during the term of the SLA.
Initial Operational Capability (IOC)	A system reaches IOC when the application has been loaded, tested, and opened to user base for production.
Initial Operating Environment (IOE)	A system reaches IOE when accepted proposals/LEs have IT assets that have progressed successfully through DISA CSD implementation and have been turned over to the partner to load their application(s) and data.
Interactive Availability	Partner availability to access the DISA CSD controlled portion of the network/system during the interactive window.
Interactive Response Time	The time from receipt of a partner-generated transaction at the DISA CSD WAN node, to which the partner is connected, until the response to that transaction from the partner's DISA CSD-resident application reaches that same WAN node. The response time on the partner-owned Local Area Network (LAN) is specifically not included since it is outside of DISA CSD control. Good interactive response times also presuppose an efficiently designed partner application.

Term	Description
Interactive Window	The period of time when interactive processing capability is available to the partner.
Invoice	A detailed listing of the type and quantity of services used by the partner for the period of time indicated, and the related charge to the partner for those services.
Mandatory Information Assurance Guidance (MIAG)	The purpose of the MIAG is to establish an acceptable security posture for assets desiring to connect to the CSD enclave. It spells out the percentage of acceptable open findings for connectivity.
Modification	Changes to existing terms and provisions of the SLA.
Non-Cancelable Obligation	Obligations incurred by DISA CSD under the current SLA that cannot be rescinded.
Operating Environment (OE)	The operating system on the server, i.e. Windows, Linux or Unix
Partner	The service or agency for which DISA CSD supplies information processing services.
Planning Estimate (PE)	An estimate project cost for services provided to a partner each fiscal year. (Oct – Sept)
Recovery Point Objective (RPO)	A point in time to which data must be restored. This is the maximum acceptable level of data loss.
Recovery Time Objective (RTO)	A period of time within which data must be restored – in other words, how long until data is available.
Standard Form 1080 (SF 1080)	Voucher for Transfers Between Appropriations and/or Funds.
Service Level Agreement (SLA)	An agreement between DISA CSD and the partner purchasing a service. At a minimum, an SLA details the type of each service to be delivered.

Term	Description
Standard Operating Environment (SOE)	A standardized enterprise software suite comprising a three-tiered architecture: Base Operating System, Core Services and Application Services.
Trusted Computer System	A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of Sensitive or Classified information.
Virtual Private Network (VPN)	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

APPENDIX C – REFERENCES AND CITATIONS

Both parties shall comply with directives, instructions, regulations, and guidance issued by the DoD including, but not limited to:

- 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
- DISA Instruction 630-230-19, March 2007, Automatic Data Processing, Information Assurance (IA) https://workspaces.disa.mil/gm/document-1.9.227275/di63023019.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.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

APPENDIX D – PERFORMANCE STANDARDS

These performance standards are available to all DISA CSD partners.

DISA CSD shall make a good faith effort to meet or exceed the following operational objectives. Circumstances beyond DISA CSD control (i.e. commercial power outages, natural disasters, inefficient application software releases, partners' local communications problems, etc.) are excluded. DISA CSD will take prompt corrective action when these objectives are not being met.

Service	Service Objective	Service Description
Interactive Availability	98.5% availability	Portion of network/system controlled by DISA CSD available to the partner during the interactive window.
Batch Throughput (mainframe)	95% or better completion rate and delivery	Completion rate and delivery by specified time during the batch window specified in the SLA. Partner initiated batch-processing outside the batch window will be processed as resources permit.
Job Failure Notification	Within 30 minutes	During normal working hours. Notification will be made after duty hours as requested by the partner.
Data Retrieval Services	15 Minutes 4 Hours 36 Hours	Tape, on-site (mount) Tape, off-site (local) Tape, off-site (backup site)
Capacity Utilization Reports	Monthly	Provides previous month's capacity data for DISA CSD-provided processing hardware.
Web-Based Invoices	Bi-weekly	Billing amounts charged to MIPRs at the service level.

DISA CSD also now offers System Network Availability Performance Service (SyNAPS) as an end-to-end monitoring tool to enhance the currently available performance monitoring tools.

Computing Services Directorate

Service Level Management

(303) 224-1660, DSN 926