Defense Information Systems Agency
Department of Defense

Defense Information Systems Agency

Computing Services Directorate (CSD)

CATALOG of SERVICES

Published Date:
14 APRIL 2009

Version 2.0

delivering applications to ...

1 force

DISA

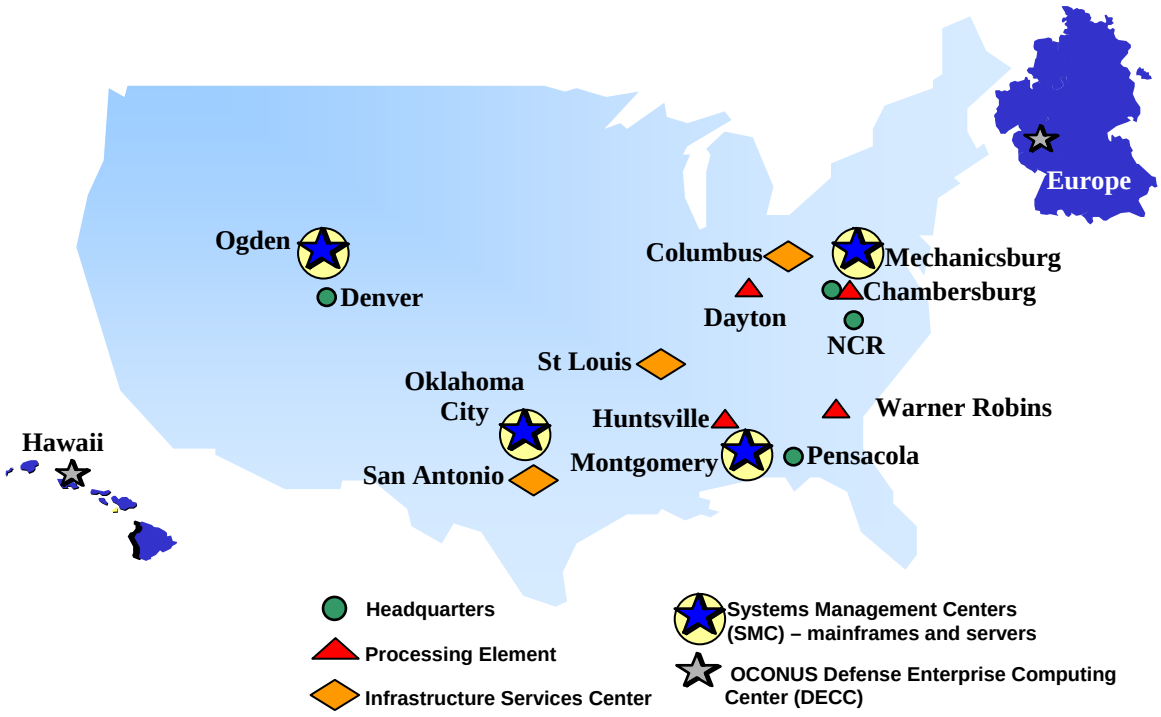
Computing Services

DISA 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 Customer 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) with a mission to deliver computing information products and services that enable and enhance the ability of Customers/end users to execute their missions.

CSD Footprint



This Catalog of Services 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 Customer systems/applications (Section 1.0), and various other services which DISA CSD makes available (Section 2.0).

DISA CSD has adopted the Information Technology Infrastructure Library (ITIL) 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

Our process improvement efforts in Service Level Management (SLM) in particular will lead to changes in this catalog that will provide more information regarding services and DISA CSD's various methods of "doing business." Major changes/additions included in this version include:

1) An expanded discussion, in Section 1.3, of the IT security provided in the DISA CSD Defense Enterprise Computing Center (DECC) environments.

2) A totally revised Section 1.4 which discusses the CSD Information Technology Service Continuity Management (ITSCM) Program (COOP). This was formerly titled "Business Continuity." The intent is to make it much easier to understand what ITSCM capabilities DISA CSD offers both as a basic service and as optional services.

3) An expanded Section 3.0 which discusses Performance Standards and Metrics applicable to DISA CSD operational performance. Watch for this section to grow and improve over the coming months and near-term version changes.

4) A new "Part II" which will include various discussions of selected DISA CSD processes that should be of interest to those partnering with us. Initially included in this version are:

   a) DoD Information Assurance Certification and Accreditation Process (DIACAP) control support provided by DISA CSD

   b) High-level DISA CSD Change Management process

   c) Process for providing cost estimates for new/additional Customer workload

   d) Server sizing

   e) Host Based Security System (HBSS)

   f) GIG Content Delivery Service (GCDS)

   g) Web-based Service Level Agreements (SLAs) – the DISA CSD Partner Portal

The following list of contacts is provided for your convenience:

CHIEF, CUSTOMER RELATIONS MANAGEMENT DIVISION: Col. Joseph Means (USAF)
(703) 681-2266 (DSN 761)
Joseph Means@disa.mil

Customer Management Executives (CMEs):

CME for DFAS/DLA/BTA/US TRANSCOM: Mr. Mark Foster
(717) 267-9175 (DSN 430)
Mark Foster@csd.disa.mil

CME for ARMY: Loyd (Lou) Morgan
(703) 681-2710 (DSN 761)
Lou.Morgan@disa.mil

CME for MHS/TRICARE: Mr. Scott Baker
(334) 416-5894 (DSN 596)
Scott Baker@csd.disa.mil

CME for JOINT STAFF/COCOM/OSD/DoD/DISA & CLASSIFIED: Mr. Robert (Bob) Plummer
(703) 681-2267 (DSN 761)
Robert.Plummer@disa.mil.

CME for AIR FORCE: Ms. Kimberly Schneider
(703) 681-2182 (DSN 761)
Kimberly.Schneider@disa.mil

CME for NAVY/MARINE CORPS: Mr. Paul Crumbliss
(703) 681 - 2181
Paul.Crumbliss@disa.mil

DISASLA@csd.disa.mil

OR

DISA CSD SLA Hot Line: (303) 224-1660 (DSN 926)

TABLE OF CONTENTS

PART I

PART II

1.0 CORE SERVICE OFFERING

DISA provides mature/standardized operations process, centralized management and Customer-focused support. DISA CSD provides a process driven heterogeneous environment to include mainframe (IBM and UNISYS), server and storage support. This section assumes all work is performed in the DISA CSD computing centers.

Services include processing and storage support; management for IBM and UNISYS mainframes; and management for Unix, Windows and Linux servers. DISA CSD executes full cost recovery charging methodologies to support these operating environments (OEs). These methodologies consist of a rate-based and reimbursable recovery approach. All Customers operating in a DISA CSD DECC receive Basic Services, as required, as part of basic rates/reimbursements.

Functions included in the Basic Services rates are:

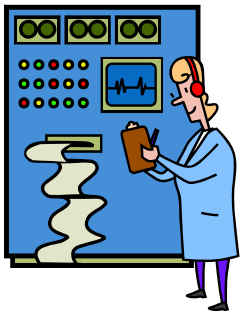
- System Administration, including but not limited to:
  - Monitor the operating status of DISA CSD production systems, including IBM, UNISYS and server based operating systems
  - Manage user accounts (operating system only)
  - Install executive software, application software, and associated patches
  - Tune operating system kernel parameters to optimize performance
  - Install and maintain the server security environment
  - Ensure compliance with Security Technical Implementation Guides (STIG) and Information Assurance Vulnerability Alert (IAVA)
  - Monitor system logs
  - Schedule backups for system files
  - Resolve referred trouble tickets
  - Develop standard solutions and procedures for the DISA CSD Knowledge Management System in accordance with standard central procedures and guidance
  - Monitor and act as liaison for the Customer for any and all changes in the system that may impact Customer production
- Security. DISA CSD provides world class computing centers with the added benefit of enjoying the high level of physical security afforded by being located on military-controlled installations. DISA CSD also provides a superior Information Assurance (IA) environment. In the transition to DIACAP, DISA CSD has accepted inherited controls for a wide range of IA responsibilities and functions. These may be seen in detail in Part II, Section 1.0, of this Catalog of Services.
- Data Communications.
- Maintenance for the standard suite of Enterprise System Management (ESM) software DISA CSD uses to monitor and manage the operating environment.
- Software products such as the operating system, ESM tools, and core software. Software required beyond these products will be charged to the Customer outside of the Basic Services rates.
- Basic level of service from the Operating Support Teams (Service Desks). See Part I, Section 1.3 of this Catalog of Services for details.

1.1 PROCESSOR SERVICES

1.1.1 IBM Mainframe

Additional Basic Services **Click for current rates**

Every IBM mainframe Customer will receive Assured Computing services developed in the DISA CSD IBM Mainframe Service Continuity Strategy. The service continuity strategy for IBM mainframe applications involves the use of a dedicated and available infrastructure and replicated data, which can be moved to an online status within the timeframes mandated for the MAC II level.



Beginning in Fiscal Year 2010 the Mainframe Internet Access Portal (MIAP) will be the DISA CSD standard data transmission tool and will be provided at no additional cost.

Capacity Planning - a standard service offering to ensure appropriate system resources are available to meet standard processing requirements and project potential changes in processing resource requirements. Capacity reporting at the OE level confirms current resource usage trends. DISA CSD collects and retains all this usage data and produces summarized reports for Customers.

Optional Services

Optional services are available upon Customer request and will be charged directly to the Customer, in addition to any costs associated with rate-based services. Optional services include:

- Dedicated Logical Partition (LPAR)
- Application Support. The term application support applies to a Customer's production/test application and not the processing environment's operating system application. 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 systems alerts. Using instructions developed by technical support and applications support, applications support personnel manage database and application environments, including recovery procedures. These rates consist of the labor costs of the technicians.
- Dedicated IBM Mainframe Management

1.1.2 UNISYS Mainframe

Additional Basic Services **Click for current rates**

Every Unisys mainframe Customer will receive Assured Computing services developed in the DISA CSD Unisys Mainframe Service Continuity Strategy. The service continuity strategy for Unisys mainframe-based applications involves the use of a dedicated and available infrastructure and replicated data, which can be moved to an online status within the timeframes mandated for the MAC II level.

Capacity Planning – a standard service offering to ensure appropriate system resources are available to meet standard processing requirements and project potential changes in processing resource requirements. Capacity reporting at the operating environment level confirms current resource usage trends. DISA CSD collects and retains pertinent usage data and produces summarized reports for Customers.

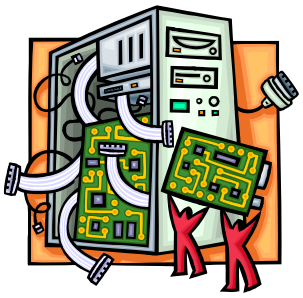
Optional Services
Optional services are available upon Customer request and will be charged directly to the Customer in addition to any costs associated with rate based services.

- Dedicated Partitions
- Application Support. The term application support applies to a Customer's production/test application and not the processing environment's operating system application. 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 systems alerts. Using instructions developed by technical support and applications support, applications support personnel manage database and application environments, including recovery procedures. These rates consist of the labor costs of the technicians.
- Dedicated Unisys Mainframe Management

1.1.3 Server

Additional Basic Services **Click for current rates**

The basic server service consists of four cost components: system administration, information security, maintenance for software that falls within the DISA CSD Standard Operating Environment (SOE), and shared communication. The Information Security (InfoSec) component consists of the labor to track the Information Assurance Vulnerability Alerts (IAVAs) and patches required to keep the OE secure.



In addition, the server basic rate includes maintenance for SOE tools other than the ESM tools. The ESM tools allow DISA to monitor and manage the OE, detect certain network errors, and determine when system-level thresholds have been exceeded. The standard monitoring software includes monitoring at the operating system level, but not at the application level (note that the initial license costs for the ESM and other SOE software products are charged as one-time implementation costs).

The shared communications component consists of the costs associated with supporting the telecommunications infrastructure that allows end-users to access their data. This consists of labor and non-labor costs.

Based on the number of sockets installed in each OE, it has its own set of rates based on the size (mini, small, medium, large, and enterprise) and type of operating system (Windows or Unix).

Optional Services

Because different Customers require different levels of support, DISA CSD provides choices from the following supplemental services. Each service has its own set of rates, based on the size (mini, small, medium, large, and enterprise) and type of operating system (Windows or Unix), as outlined in the paragraph above.

- Hardware Services

  These services are required for DISA owned/DISA maintained hardware. It is not required if the hardware is Customer owned/Customer maintained. This rate consists of hardware and software maintenance and depreciation, amortization, cables, interface cards, and other miscellaneous items required to keep the server reliably operational. (The agreement between DISA-provided vs. Customer-provided hardware must be determined before a price estimate is provided to the Customer by DISA. Once accepted by the Customer, that agreement will be the basis for implementation and sustainment of the Customer's workload.) Capacity Planning is also included in the hardware services offering. This service is to ensure appropriate system resources are available to meet standard processing requirements and project potential changes in processing resource requirements. Capacity reporting at the operating environment level confirms current resource usage trends. DISA CSD collects and retains pertinent usage data and produces summarized reports for Customers. Customers who maintain their own hardware (and thus do not pay the Hardware Services rate) may avail themselves of Capacity Planning at a cost of ten (10) percent of the Hardware Services rate for their suite of hardware.

- Application Support

  The term application support applies to a Customer's production/test application and not the processing environment's operating system. 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 the technical support staff and the functional community, applications support personnel manage database and application environments, including recovery procedures.

  Application support personnel are Customer service professionals in the Operation Support Team (OST) who possess more extensive knowledge of various software, hardware, and communication specialties than entry-level Customer Support Personnel (CSP). 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/errors
  - Building and maintaining schedules
  - Coordinating with the database administrators and system administrators on new and/or changed releases
  - Associating security profiles to jobs

- Monitoring backups
- Mitigating contention and/or improving application performance
- Coordinating with Customers on service interruptions
- Managing, coordinating, and installing application releases
- Managing reports (for example, using software such as Certification Authority [CA] Dispatch)
- Monitoring job schedules
- 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 instances and for some workloads)

- Database Administration

  These rates consist of (1) the labor costs of the database administrators supporting any database management systems that run on Unix or Windows platforms and (2) the costs of database management tools that improve their productivity. An example of the latter is Quest software, which automates or simplifies many labor-intensive tasks. Database administrators at operating sites manage a variety of database environments functions including but not limited to:

  - Set up of database structures
  - Allocation of space
  - Creation or modification of database instances
  - Compliance with Security Technical Implementation Guides (STIGs)
  - Scheduling of backups for data files
  - Resolution of referred trouble tickets
  - Development of standard diagnostic, problem resolution, operations, and maintenance procedures for the DISA CSD Knowledge Management System

- Oracle Database Software Maintenance

  The Oracle database management system is the current database application of choice in the DISA CSD environment. DISA CSD has established a rate for Oracle database software maintenance. This rate consists of the maintenance costs of the Oracle database software only. Any other database software maintenance is considered cost-reimbursable and not covered by these rates. The initial cost of the Oracle license(s) is considered a one-time implementation cost.

- 24 x 7 System Administration

The Basic Services rate provides for on-site system administration Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. For those workloads requiring 24x7 on-site system 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 Database Administration

  The standard Database Administration rate provides for on-site database administration Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. 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

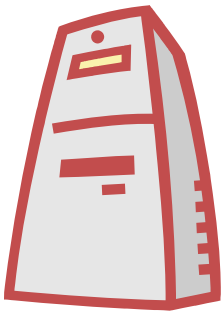
  The standard Application Support rate provides for on-site application support Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. For those workloads requiring 24x7 on-site 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 we haven't established rates for every conceivable service a Customer may request, we handle unique requests on a cost-reimbursable basis. For these offerings we charge the direct cost, plus all indirect and general and administrative costs. This list represents some of the cost-reimbursable services we provide to our Customers, but it is far from exhaustive.

- Non-standard operating systems, 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), 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.
- Certain Customer-owned servers that DISA maintains.
- Certain extremely large OEs that would skew the rates if left within the rates.

1.1.4 IBM Mainframe zLinux (A new offering beginning in Fiscal Year 2010)



In FY10, DISA CSD will begin to offer a new service called zLinux, which will run the Linux operating system on special mainframe hardware. This mainframe hardware (called an Integrated Facility for Linux (IFL) engine) is specifically designed by IBM to run Linux workloads. DISA CSD will use a zLinux rate to charge Customers by measuring the amount of processing time their workload uses (based on CPU hours). Storage services for the zLinux environment will be charged using the server storage rates method, and the zLinux service will have the functions listed in the Basic Services under 1.1 Processor Services. In addition, the following Basic and Optional Services will be offered.

zLinux

Additional Basic Services

The zLinux Customer will receive in the Basic Services the use of a shared Continuity of Operations Processor at a remote site for disaster recovery; however, this does not include any of the storage required for continuity of operations. The Customer would need to purchase additional storage services as outlined in Section 1.4 Service Continuity in order to be able to use the shared Continuity of Operations Processor at the remote site.

Optional Services

Because different Customers require different levels of support, DISA CSD provides choices from the following supplemental services. Each service has its own set of rates; however, if a Customer has a uniquely large workload, DISA CSD will work with the Customer to develop an agreeable labor support cost method outside of these rates.

- Application Support
  The term application support applies to a Customer's production/test application and not the processing environment's operating system. 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 the technical support staff and the functional community, applications support personnel manage database and application environments, including recovery procedures.

  Application support personnel are Customer service professionals in the OST who possess more extensive knowledge of various software, hardware, and communication specialties than entry-level CSPs. 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/errors
  - Building and maintaining schedules

- Coordinating with the database administrators and system administrators on new and/or changed releases
- Associating security profiles to jobs
- Monitoring backups
- Mitigating contention and/or improving application performance
- Coordinating with Customers on service interruptions
- Managing, coordinating, and installing application releases
- Managing reports (for example, using software such as CA Dispatch)
- Monitoring job schedules
- 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 instances and for some workloads)

- Database Administration
  These rates consist of (1) the labor costs of the database administrators 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 Quest software, which automates or simplifies many labor-intensive tasks. Database administrators at operating sites manage a variety of database environments functions including but not limited to:

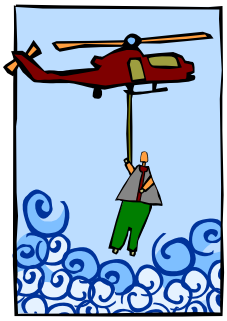
  - Set up of database structures
  - Allocation of space
  - Creation or modification of database instances
  - Compliance with STIG's
  - Scheduling of backups for data files,
  - Resolution of referred trouble tickets
  - Development of standard diagnostic, problem resolution, operations, and maintenance procedures for the DISA CSD Knowledge Management System

- 24 x 7 System Administration
  The Basic Services rate provides for on-site system administration Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. For those workloads requiring 24x7 on-site system 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 Database Administration
  The standard Database Administration rate provides for on-site database administration Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. 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 Monday through Friday from 0800 to 1600. It also includes a two (2) hour response to emergencies on nights and weekends and weekend scheduled maintenance once a month on average. 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. In the event that a Customer wishes a greater degree of protection, the Customer may pursue a strategy of placing additional equipment at the production site and having that equipment pre-configured and available to serve as a local fail-over environment. Please note that local fail-over will not satisfy the COOP requirements detailed in DoD Instruction 8500.2, which mandates a remote recovery strategy at a predetermined location.

If a local failover option is pursued, the additional costs must be negotiated with input from the Business Service Management Center.

The information and offerings available for satisfying COOP (remote recovery) requirements are detailed in Section 1.4.

1.2 STORAGE SERVICES

Click for current rates

Storage rates are platform specific (IBM, UNISYS, and Server). Discussion of each follows.

1.2.1 IBM Mainframe Storage

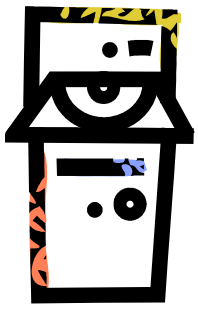
IBM mainframe storage is provided and billed for all IBM workload to include the Assured Computing component. Please see discussion in paragraph 1.1.1.

1.2.2 UNISYS Mainframe Storage

UNISYS mainframe storage is provided and billed for all UNISYS workload to include the Assured Computing component. Please see discussion in paragraph 1.1.2.

1.2.3 Server Storage

Server Customers are offered a wide array of storage opportunities that allows DISA CSD to provide the level of service required for all MAC levels, including MAC level I applications/systems.



Basic Service

DISA Customers will be invoiced for ALL appropriate costs based on the service selected and the amount of allocated storage in gigabyte (GB)/month. All Customers will be provided and invoiced the Basic Service Level L1 in the table below for data recovery, not application restoration. Customers may select to augment the Basic Service in accordance with their needs and MAC level. If a Customer 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 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	
		OST Support	
.Backup Services		Standard weekly Operational Backup (1 copy onsite, retained 4 weeks) designed for local recovery only.	
		Incremental daily Operational Backups (retain 2 weeks onsite) designed for local recovery only.	
		Standard weekly COOP Backup (1 copy offsite, retained 4 weeks) designed for remote recovery.	
Data Center Services		Security	
		Facilities	
		Networks	
		Tech Refresh (Storage Array)	
		Help Desk	

Optional Storage Levels

Rate-Based

Rate-based server storage pricing is based on the GB (raw) storage used per month and the level of service requested by the Customer 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 COOP 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

Default Local

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.

Optional Offerings

- **Local/Operational 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.
  - **Advanced Local/Operational Recovery: Combination 1**

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.

- **Advanced Local/Operational Recovery: Combination 2**

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.

- **Advanced Local/Operational Recovery: Combination 3**

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.

Overview of Operational 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.

Offerings related to remote recovery as part of a Service Continuity/COOP strategy are addressed in Section 1.4.

Cost Reimbursable Services include:

- 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

1.3 SERVICE DESK (OST) SUPPORT

DISA CSD offers a wide range of technical support through Customer-centric service and agency specific Operating Support Teams (OSTs).

Basic Services

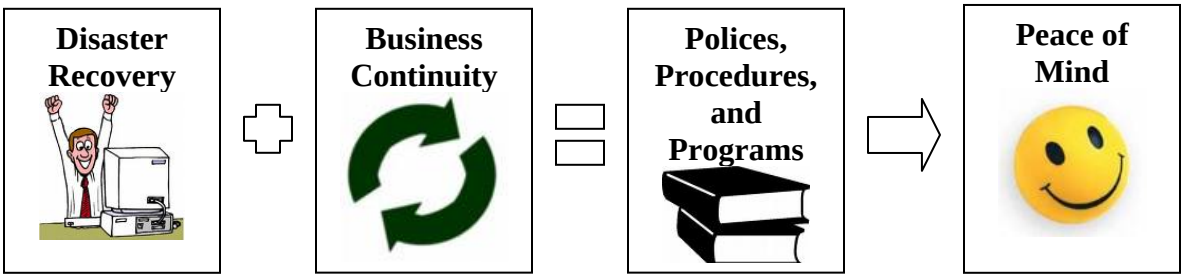
- **Level 2 -** This is the level of Service Desk support that DISA extends to all its Customers and is included within the basic rates. These services consist of those usually associated with a Level 2 Help Desk.
  Password resets are included in this category since generally an end-user calls their own Service Desk first and is then redirected to the DISA OST, which authenticates the callers and resets the password.

Optional Services

- **Level 1 -** Refers to a Service Desk that takes on the added responsibilities (phone calls, faxes, e-mails, etc.) coming directly from the end-users. With the exception of password resets (as discussed above), these costs are additional and will be billed directly to the Customer requesting the service in addition to any other rate-based charges.
- **Level 3 -** Refers to a Service Desk that possesses intimate knowledge of a given business (such as logistics, accounting & finance, security, health care, etc.), software package (e.g., SAP), or other subject matter. This level of support will be billed directly to the Customer requesting the service in addition to any other rate-based charges.

1.4 SERVICE CONTINUITY

Disaster recovery and business continuity are the policies, procedures and programs put in place to allow DISA CSD, in concert with Customer personnel, to provide an effective level of assurance that workloads will continue to process in accordance with known regulatory requirements.



The creation of data backups is addressed later in this section. The basic rate for storage includes the creation of tape backups that are kept on-site and off-site to facilitate operational recovery at the primary production site. Any additional coverage, including recovery at a remote facility following a severe outage or disaster, must be specifically addressed as part of the SLA negotiations.

When a Customer selects a desired level of data protection, they must also select the appropriate corresponding infrastructure to facilitate the desired recovery. This is especially true for server-based computing.

By contracting with DISA for Service Continuity/COOP services, the Customer also gains the option of requesting exercises of that coverage using the processes and/or environments that would be used for an actual recovery. There are two primary types of exercises, table-top and simulation.

In a table-top exercise, the personnel who would be involved in an actual recovery gather together and walk through the processes developed for that recovery. This can be accomplished in person or through the use of teleconferences and/or videoconferences. The time to complete a table-top exercise will be dependent on the scope and coordination requirements associated with the exercise. It can be as little as a few hours or as much as several 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.

In all cases, any charges associated with traveling to or shipping to the recovery site will be the responsibility of the Customer requesting the exercise. Shipping is typically restricted to backup tapes and documentation required to conduct the exercise. Travel costs are usually limited to the costs associated with temporary duty (TDY) of DISA personnel.

In cases where Customers decline coverage for service continuity, no storage or infrastructure will be provided for anything beyond operational recovery. In addition, DISA CSD personnel will not develop recovery procedures for those applications. Customers will be expected to assume full responsibility for protecting those applications in accordance with established regulatory requirements.

The table below shows the options available for Service Continuity/COOP, or remote, data recovery. Please note that in order to recover an application, processing platforms must also be available at the remote site. The chart immediately below addresses the storage options only. See the discussion on the following pages which describes the Remote Recovery Combinations (RRCs) that are available. Note that in order to have a recovery option that meets the COOP requirements detailed in DoD Instruction 8500.2, appropriate selections must be made for both storage (data) recovery and server (processor) recovery. As noted previously, the Assured Computing environment will meet MAC II requirements (processor and data) for IBM or UNISYS mainframe applications.

Level	MAC Level	Description	Maximum Data Loss
R1	MAC III	Basic Remote	<7 Days
R2	MAC II	Operational Remote	<24 Hours
R3	MAC II	High-Availability Remote	<8 Hours
R4	MAC I	Non-Disruptive Remote	<1 Second

- **Geographically Remote Recovery:** Geographically remote recovery differs from an operational recovery in that it assumes the primary processing environment is no longer operational or no longer accessible. In that situation, the only alternative is to cease processing until the primary environment is available or to move the processing to an alternate location. The following entries/offerings will deal with DISA offerings associated with that remote recovery strategy.

  - **Remote Recovery: Combination 1 (RRC 1)**

RTO = 5 days RPO = 7 days

This level of continuity provides a secure processing environment with sufficient storage infrastructure in place to allow a remote recovery with an RTO of five (5) days and an RPO of seven (7) days. The RTO timeline is driven by the use of tape-based backups to restore all required backup data to storage capacity pre-positioned at the recovery site. The RPO is driven by the frequency of backups stored off-site from the primary processing facility.

If daily incremental backups are stored off-site and are available for restoration, an RPO of 24 hours is achievable. If the only tapes off-site are weekly full volume backups with no corresponding daily incremental backups, then the RPO could be as high as seven (7) days. Any increase in frequency of backups will result in a corresponding reduction in the maximum

RPO available to the Customer, but will also typically result in an increased charge to the Customer.

For this level of recovery to be effective, a corresponding hardware and software infrastructure needs to be available and operational at the remote recovery site. This approach is also referred to in some areas as “hot site failover” and is designed to use shared resources at a single site to provide continuity for production requirements.

Because the shared resources are designed to be used by multiple sites running various applications for multiple Customers, the resources are installed in a fairly “vanilla” configuration. Upon notification that an outage has occurred, DISA personnel will begin customizing and configuring the infrastructure to accommodate the incoming processing.

Upon the restoration of the primary production facility, the processing will be removed from the remote recovery site and returned to the primary site. At that point, the shared resources will be returned to their default configuration.

- **Remote Recovery: Combination 2 (RRC 2)**

This level of continuity provides a secure processing environment with sufficient storage infrastructure in place to allow a remote recovery with an RTO and an RPO of 24 hours. The timeline is driven by the use data backups stored at the remote recovery site in combination with dedicated and pre-configured server resources available there. For this option to be effective, it requires the Customer to select not only the appropriate storage option, but also the appropriate remote dedicated processor offering. By having dedicated and pre-configured equipment in place, the required RTO and RPO targets are achievable.

- **Remote Recovery: Combination 3 (RRC 3)**

This level of continuity provides a secure processing environment with sufficient storage infrastructure in place to allow a remote recovery with an RTO and an RPO of eight (8) hours. The timeline is driven by the use data backups that are taken more frequently and stored in an online status at the remote recovery site in combination with dedicated and pre-configured server resources available there. For this option to be effective, it requires the Customer to select not only the appropriate storage option but also the appropriate remote dedicated processor offering. By having dedicated and pre-configured equipment in place, the required RTO and RPO targets are achievable.

- **Remote Recovery: Combination 4 (RRC 4)**

This level of continuity provides a secure processing environment with sufficient storage infrastructure in place to allow a remote recovery with an RTO of 30 minutes and an RPO of less than one (1) second. The timeline is driven by the use of data replication to create near-instantaneous backups stored in an online status at the remote recovery site. This approach, in combination with dedicated, pre-configured and operational server resources, can provide assurance of minimal processing interruption with virtually no data loss.

For this option to be effective, it requires the Customer to select the appropriate storage option and an infrastructure to be resident at the recovery site that can be brought online in less than 30 minutes. Any hardware solution for recovery requirements this stringent will be developed as a customized solution.

Overview of Remote Recovery Combinations

Options	MAC Level	Description	Storage Offering	Processor Offering	RTO/RPO
Remote Recovery Combination 1	MAC III	Remote recovery using tape-based data backups and shared processing capability at a designated recovery site	Basic Remote	Shared COOP	RTO <5 Days, RPO <7 Days
Remote Recovery Combination 2	MAC II	Remote recovery using backup data stored at the recovery site and pre-configured processing capability	Operational Remote	Dedicated COOP	RTO & RPO <24 Hours
Remote Recovery Combination 3	MAC II	Remote recovery using backup data stored at the recovery site and in an on-line state as well as pre-configured processing capability	High-Availability Remote	Dedicated COOP	RPO & RTO <8 Hours
Remote Recovery Combination 4	MAC I	Remote recovery using near-synchronous replication of data stored at the recovery site and in an on-line state as well as dedicated, pre-configured and operational processing capability	Non-disruptive Remote	Dedicated COOP	RPO <1 Sec, RTO <30 Min

Note: All options for remote recovery rely on a combination of designated infrastructure and available backup data.

Customized Fail-Over

It is possible that mission requirements for a particular application, or suite of applications, is not adequately addressed by any of the standard Remote Recovery Combinations defined above. For example, it may be that a workload balanced production environment is in place and the desired COOP solution is to have the environment sized and configured to absorb the loss of one or more elements of the environment. Assuming that the sites are geographically separate, that would be a feasible solution. If the Customer does determine that a fail-over solution is desired and that the pre-defined approaches are not adequate or preferred, then a customized fail-over solution can be developed and implemented. Any solution of this type must be identified within the relevant SLA and supporting documentation must be appended to or referenced within that SLA.

Test & Development (T&D) Solutions

This approach is used in some instances where DISA provides and supports both a production environment and an associated T&D environment for a specific application. For this approach to be a valid solution the two environments MUST be in geographically separate locations and the T&D environment must be appropriately sized to serve as a COOP solution for the production site. Any solution of this type must be identified within the relevant SLA and supporting documentation must be appended to or referenced within that SLA.

Outsourcing Continuity Services

In some cases, a DISA Customer may choose to outsource their continuity requirements to an alternate provider or it may be a responsibility assumed by the Customer using their own internal resources. Any Customer who is not contracting with DISA for Service Continuity/COOP services is excluded from the DISA program. No promise or expectation of Service Continuity/COOP is implied or should be inferred. The SLA will include an annotation that the Customer has “No COOP” requirements that are to be satisfied by DISA.

The creation of recovery procedures will only be accomplished for those applications for which DISA has recovery responsibility. Procedures designed to be used by an alternate provider or by the Customer 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.

All backup programs used by DISA for data replication as well as tape-based backups are designed to serve multiple Customers. It is possible that a Customer may require unique individual backups to be used in a recovery by parties other than DISA. In these situations, our standard backup approach is not designed to satisfy the request. If a Customer needs non-standard data backups, they will be responsible for reimbursing DISA for the associated cost.

2.0 OTHER SERVICES

While the primary mission of DISA CSD is to host and manage military service and defense agency computing systems and applications, there are also several related areas in which DISA CSD can provide support. A discussion of those capabilities follows.

2.1 RAPID ACCESS COMPUTING ENVIRONMENT (RACE)

This is the perfect opportunity to allow you to test your application in a DECC-like environment. DISA provides hosting, networking, security and connectivity, and offers the package to Customers as a service. RACE is available to all CSD Customers, including all Services and Agencies as well as their corporate design partners. Users are able to 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.

This is a service that allows authorized customers to provision virtual servers using drop down menu selections on a web portal, and have the server available for use by the next business day. The server image resides on a virtual server host in a DISA DECC facility. The server images are designed to be flexible design platforms to support web, application and database development environments. The server images function as dedicated servers. The standard package includes a Central Processing Unit (CPU), one (1) GB memory, 50 GB disk storage, and Internet Information Services (IIS) for Windows-based servers or LAMP (Linux, Apache, MySQL and PHP) for Red Hat servers. Other combinations of CPU/Memory/Storage are available.

2.2 COMMUNICATIONS SERVICES

DISA CSD has network monitoring tools at our disposal to provide outstanding service for our Customers. It is the joint responsibility of DISA Network Services and DISA CSD to provide and maintain the Global Information Grid (GIG) utilized by Customers. Non-classified Internet Protocol Routing Network (NIPRNet) availability is built into the system via hardware and circuit redundancy throughout the Wide Area Network (WAN).

DISA CSD is responsible for a separate subnet used to support DECC connectivity and applications. The same degree of circuit and hardware redundancy is provided to support the same degree of survivability.

Basic Services

The communications component consists of the costs associated with DISA internal communications infrastructure and support teams. This infrastructure allows end-users, anywhere in the world, to connect safely and securely to the data that resides within our processing centers. These basic services are billed by a surcharge to IBM CPU Hour, UNISYS Standard Units of Processing (SUP) and in Server, are included in the Server basic rates.

Optional Services

Additional WAN communications requirements may be handled directly with the DISA Combat Support Directorate (DISA-GS) via the standard Service Request Form (SRF). These costs are additional and will be billed directly to the Customer requesting the service in addition to any other rate-based charges.

Data Transmission Options

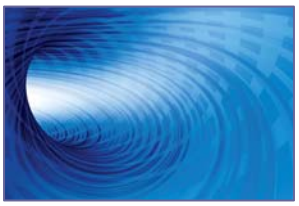
DISA will provide a variety of options to satisfy data transmission requirements. These services (except for Mainframe Internet Access Portal [MIAP]) are additional and will be billed directly to the Customer requesting the service in addition to any other rate-based charges. The following table describes each of the options.

Traffic Flow	Solution to Use	Notes
Site-to-site VPNs	Varies	
.com -> .mil (DECC)	B2B	Complete B2B/VPN checklist and follow instructions enclosed.
.mil -> .mil (DECC)	PB Collo	If customer is collocated at DMZ, use customer equipment. If customer is not collocated at DMZ, use DISA provided Cisco 7200. Complete B2B/VPN checklist and follow instructions enclosed.
.mil (DECC) -> .mil (DECC)	Inter-DECC VRF	No configuration needed
Any .com or .mil -> .mil (DECC) that is proxiable and is required to be proxied based on PPSM and associated boundaries	DMZ Proxy	Firewall rules need amended in customer context on DMZ FW for required ports below.
Ports 20,21 – FTP (User initiated)	MIAP	Complete MIAP application online
Ports 20,21 – FTP (Batch initiated)	B2B or PB Collo & GEX (on the backside)	Complete B2B or PB Collo checklist as well as the GEX checklist and submit to Theresa Walker theresa.walker@disa.mil
Port 22 – SSH/SFTP	GEX	Complete GEX checklist and submit to Theresa Walker theresa.walker@disa.mil
Port 23 – Telnet	MIAP	Complete MIAP application online
Port 25 – Email	Mail Relay Services	Complete Mail Relay checklist and submit to Theresa Walker theresa.walker@disa.mil
Port 80 – HTTP	Web Proxy	Complete WebDMZ checklist and submit to Theresa Walker theresa.walker@disa.mil

Port 443 – HTTPS/SSL	Web Proxy	Complete WebDMZ checklist and submit to Theresa Walker theresa.walker@disa.mil
Port 1414 – MQ Series	GEX	Complete GEX checklist and submit to Theresa Walker theresa.walker@disa.mil
.mil (DECC) -> .com or .mil on TCP port 80 or 443	DMZ Forward Proxy	No configuration needed above DMZ VPN Router (top side of 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 rules need amended in Non Proxy context on DMZ FW for required ports.

The following communication services will be included in the basic processor rates in Fiscal Year 2010 and the Customer will no longer incur an additional charge.

Business to Business (B2B) Gateway:



The DoD B2B Gateway 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. The DoD B2B Gateway is 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 Customers in the commercially accessible WAN. It also services Domain Name Server (DNS) resolution requests on User Datagram Protocol (UDP) port 53. This infrastructure is intended only for applications which require back-end NIPRNet connections, for example, database and application server accesses. It is not intended for web applications with embedded static content, which can be hosted elsewhere (Defense Technical Information Center [DTIC]), nor is it intended for applications requiring only NIPRNet access Processor Services.

2.3 WEB SERVICES

DISA CSD can provide five (5) levels of web hosting. The levels range from “simple” to “complex/custom.” The standard services are based on using Microsoft Windows Std/IIS or Linux/Apache on DISA CSD-provided hardware. The offerings are summarized as follows:

1) **Bronze, Level 1**
Simple, relatively static web sites, with no scripting support required and having small data requirements (less than 1 GB per site)

2) **Bronze, Level 2**
Simple to intermediate web sites, scripting supported by CSD and having small data requirements (less than 1 GB per site)

3) **Silver**
Intermediate sized web sites requiring a dedicated OE(s), scripting supported and increased storage requirements (5 GB of data per OE)

4) **Gold**
Intermediate to complex web sites requiring a dedicated server, scripting supported, and having a significant storage requirement (20 GB of data)

5) **Platinum**
Custom web hosting solutions which could include any or all of the following options:

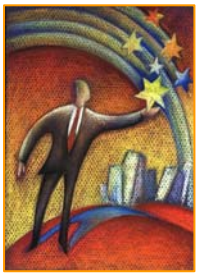
a) Many configurations possible
b) Load balancing and clustering options
c) Complete two and three-level architectures
d) Geographically dispersed mirrored environments

2.4 KNOWLEDGE MANAGEMENT

DISA CSD has been using our Knowledge Management (KM) system internally to support you, the Customer, for over four years. As a proven tool for capturing and sharing critical information and best practices, DISA will be offering a hosted, for-fee KM solution so Customers can leverage the solution for their own internal needs.

The KM tool can be tailored and rolled out quickly to your organization. This solution will help capture, organize, and locate the information your people need to be successful and efficient. The DISA CSD KM solution allows your people to work on things that matter, not searching through thousands of emails, file directories, and hard copies to find the answers they need.

The DISA CSD KM solution for Customers offers the following benefits:



- Mission Effectiveness
    - Allows your organization to focus immediately on capturing and sharing your organization's authoritative information to improve efficiency and reduce cost.
    - Provides a proven, scalable framework that can be tailored to your organization. Includes comprehensive hard copy and computer-

based training materials. DISA CSD can also provide proven best practice advice for your knowledge gathering and management activities.

- Decreases risk of critical knowledge walking out the door due to retirement, transfer, or turnover.
- Decreases time to get the answers people need, encourages collaboration on best practices, and increases time available to address other organizational challenges.

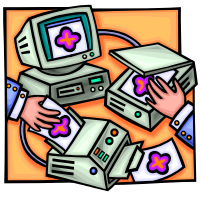
- Cost Efficiency
  - Eliminates technology acquisition, implementation, and ongoing maintenance effort and cost.
  - Leverages the same DISA CSD hosted benefits as your other applications, such as security, support, failover, and high availability.

  - Billed as a DISA CSD service, this approach eliminates additional contracts and contractor management. The DISA CSD fees are more cost effective than implementing and maintaining your own KM technology.
  - Rate-based service

2.5 CONTENT DELIVERY SERVICES

The GIG 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 servers 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 TCP optimization; object pre-fetching; persistent connections; Secure Socket Layer (SSL) off-load; and content delivery services such as caching, compression, and failover. Also, GCDS provides 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.

2.6 SYSTEM DESIGN AND INTEGRATION SUPPORT

Although the Customer is ultimately responsible for the implementation of an application along with its configuration management and baseline control, DISA CSD may provide application surveillance during implementation if requested. These functions often include many activities that contribute to the successful operation of a data system. They include, but are not limited to: assistance for initial design or modification; assistance with integration of existing and future systems; design and programming support to satisfy application security requirements; installation or deletion of application software; assistance with application implementation; and assistance with proper operation of the application. These functions ***do not*** include modification of any of the baseline production application codes, which is the responsibility of the Customer's Central Design Activity (CDA).

2.7 CIVILIAN EMPLOYEE TIME AND ATTENDANCE/PAYROLL SUPPORT

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 Customer communities within the federal government unique application support and Help Desk services currently supporting over 83,779 user accounts. The ATAAPS service is a rate-based offering (rates approved/set by the Office of the Secretary of Defense [OSD {Comptroller}], revolving funds). They are based on "per user" pricing and are billed monthly.

2.8 CUSTOMER SERVICE

DISA CSD provides focused Customer management services. The Customer Management Division is structured by the major Customer, Service or Agency. Each Customer management organization is lead by a Customer Management Executive (CME) 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 the Customer experience. During the typical project life cycle, this may include fielding initial Customer 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 Customers 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.

3.0 PERFORMANCE STANDARDS

DISA CSD shall make a good faith effort to meet or exceed the following operational objectives. Circumstances beyond DISA CSD control (e.g. commercial power outages, natural disasters, inefficient application software releases, Customer's 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 Customer 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. Customer 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 Customer.
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 – provides processing hardware.
Web-Based Invoices	Bi-weekly	Billing amounts charged to MIPRs at the service level

4.0 ACRONYMS

The following acronyms are referenced throughout this support agreement.

Acronym	Definition
AIS	Automated Information System
ASC	Application System Code
ATAAPS	Automated Time Attendance and Production System
ATO	Authority to Operate
BOM	Bill of Materials
BAN	Billing Account Number
BCP	Business Continuity Plan
BMC	Business Management Center
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
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
CONUS	Continental United States
COOP	Continuity of Operations
CPU	Central Processing Unit
CSCAPE	Computing Services Customer Automated Price Estimator
CSD	Computing Services Directorate
DAA	Designated Approving Authority
DASD	Direct Access Storage Device
DBSMC	Defense Business Systems Management Committee
DBT	Defense Business Transformation
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DIACAP	DoD Information Assurance Certification and Accreditation Process
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
DSD	Data System Designator
DSN	Defense Switch Network
ESSG	Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group
FFS	Fee-for-Service

Acronym	Definition
FIPS	Federal Information Processing Standards
FMLO	Financial Management Liaison Office
FORCECON	Force Condition
FY	Fiscal Year
GCCS	Global Command and Control Services
GCDS	GIG Content Delivery Service
GCSS	Global Combat Support Services
GIG	Global Information Grid
GNC	Global NetOps Center
GS	Combat Support Directorate
IA	Information Assurance
IAC	Invoice Account Code
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IBE	Initial Business Estimates
ICE	Interactive Customer Evaluation
IFC	Initial Functional Control
IIS	Internet Information Services
IM	Instant Messaging
IS	Information System
INFOCON	Information Condition
INFOSEC	Information Security
IOC	Initial Operational Capability
IP	Internet Protocol
IRB	Investment Review Board
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Management
LAN	Local Area Network
LPAR	Logical Partition
MAC	Mission Assurance Category
MIAP	Mainframe Internet Access Portal
MIPR	Military Interdepartmental Purchase Requests
NDAA	National Defense Authorization Act
NIPRNet	Non-Classified (but Sensitive) Internet Protocol Routing Network
OCONUS	Outside of the Continental United States
OE	Operating Environment
OPM	Office of Personnel Management
O&M	Operations and Maintenance
OS	Operating System
OSD	Office of the Secretary of Defense
OST	Operations Support Team
PE	Planning Estimate
PKI	Public Key Infrastructure
PM	Program Manager
POC	Point of Contact

Acronym	Definition
RACE	Rapid Access Computing Environment
RDT&E	Research, Development, Test & Evaluation
RPO	Recovery Point Objective
RSD	Rogue System Detection
RTO	Recovery Time Objective
SCP	System Compliance Profiler
SF 1080	Standard Form 1080 Voucher for Transfers Between Appropriations and/or Funds
SFUG	Security Features User's Guide
SIPRNET	Sensitive Internet Protocol Routing Network
SLA	Service Level Agreement
SMC	Systems Management Center
SOE	Standard Operating Environment
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
T&C	Terms and Conditions
TCP	Transmission Control Protocol
TDY	Temporary Duty
TMS	Trouble Management System
UIC	Unit Identification Code
VPN	Virtual Private Network
WCF	Working Capital Funds

5.0 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 DFAS, which constitutes an official request to pay for services delivered. Bills present only summary data on charges to the Customer. 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)
Charges	Amount the Customer is required to pay for the services delivered.
Confidentiality Level	Determined by whether the system processes classified, sensitive, or public information.
Customer	The Service or Agency for which DISA CSD supplies information processing services.
Customer Account Representative (CAR)	A representative of DISA CSD who serves as the primary point of contact to the Customer for DISA CSD services. The CAR is responsible for assuring the Customer is satisfied with DISA CSD services.

Term	Description
DASD Services	Provide the Customer with daily/weekly backup of Customer data (daily incremental, daily full volume dumps, and/or data base logs).
Data Retrieval Services	Customer 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 Customers' information system requirements in the event of a disaster.
Domain Name Service (DNS)	An Internet service that translates domain names into IP addresses.
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)	Systems are ready for full production and can be turned over to Operations for sustainment.
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 Functional Control (IFC)	Racked and Stacked. The application is successfully installed and all STIGs have been applied. Customer can perform functions not on the network.
Initial Operational Capability (IOC)	Connection Approval, IATO, and checklist completed
Interactive Availability	Customer availability to access the DISA CSD controlled portion of the network/system during the interactive window.

Term	Description
Interactive Response Time	The time from receipt of a Customer-generated transaction at the DISA CSD WAN node, to which the Customer is connected, until the response to that transaction from the Customer's DISA CSD-resident application reaches that same WAN node. The response time on the Customer-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 Customer application.
Interactive Window	The period of time when interactive processing capability is available to the Customer.
Invoice	A detailed listing of the type and quantity of services used by the Customer for the period of time indicated, and the related charge to the Customer for those services.
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
Planning Estimate (PE)	An estimate project cost for services provided to a Customer 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.
Service Level Agreement (SLA)	An agreement between DISA CSD and the Customer of the service. At a minimum, an SLA details the type of each service to be delivered; the charge for each unit of service; estimated costs for rate-based and non-rate based services; and how payment will be made.
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.

Term	Description
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.

6.0 REFERENCES AND CITATIONS

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

DoD Directive 8500.1, Oct 02, Information Assurance (IA)

DoD Instruction 8500.2, Feb 03, Information Assurance Implementation
http://www.dtic.mil/whs/directives/

DoD Directive 5200.1-R, Jan 97, Information Security Program

DoD Instruction 4000.19, 9 August 1995, Interservice and Intragovernmental Support

DoD 7000.14-R, October 2002, Department of Defense Financial Management Regulation (Reimbursable Operations, Policy and Procedures-Working Capital Funds [WCF])

DoD 8510.01, November 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP)
http://iase.disa.mil/index2.html

CJCSM 6510.01, Mar 03, Defense-In-Depth, Information Assurance (IA), and Computer Network Defense (CND)

DISAI 630-230-19 DISA Information Security Program

OMB Circular A-130, Feb 96, Management of Federal Information Resources

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

Document Source

All DoD directives, regulations, circulars, and instructions
http://www.dtic.mil/whs/directives/

The OMB Circular A-130
http://www.whitehouse.gov/omb/circulars/#numerical

DoD Financial Management Regulation 7000.14-R, Volume 11B
http://www.dtic.mil/whs/directives/

DoD Instruction 4000.19
http://www.dtic.mil/whs/directives/corres/html/400019.htm

7.0 SERVICE RATES

Click for current rates

PART II

DISA Computing Services Directorate Topics of Interest

1.0 DISA CSD INHERITED DIACAP CONTROLS

CSD has documented the following IA controls as inherited. They are defined as follows:

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.
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.

Control	Control Name	Description	Supporting Rational
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.
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.

Control	Control Name	Description	Supporting Rational
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.
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.

Control	Control Name	Description	Supporting Rational
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.
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.

Control	Control Name	Description	Supporting Rational
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.
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.

Control	Control Name	Description	Supporting Rational
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.
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.

Control	Control Name	Description	Supporting Rational
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.

2.0 THE FUTURE OF "BEST PRACTICE" CHANGE MANAGEMENT AT DISA CSD

As DISA CSD moves toward improving processes using ITIL as a framework for instituting "best practices," a strong Change Management process is the keystone to success.

CSD is implementing a new Enterprise Change Management policy and process. The goal of this process is to respond to the Customer's changing business requirements while maximizing value and reducing incidents, disruptions, and re-work. The objectives of the Change Management process are to ensure changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. The current scope of Change Management covers production hardware, software, and network assets; however, through continual service improvement we plan to mature to a process that includes all assets that affect the performance of the services we provide. The following concepts are included in our Enterprise Change Management policy/process, and their execution continues to evolve in maturity. Please feel free to contact our Change Management Process Owner for more information on our new Enterprise Change Management process.

- All changes must be registered, authorized and implemented through the CSD Enterprise Change Management process.
- All changes will be coordinated through a single focal point and tool.
- A Change Request must be submitted in time for appropriate assessment prior to authorization and release implementation.
- All changes that impact service capability will be assessed for performance, risk and resources needed to implement the change. Based on the assessment, categorization will be used to identify the level of authorization required and the change lead times needed for change implementation through the Release Management process.
- The Change Manager (with input from the initiator and other stakeholders) will allocate a priority for every Change Request that is based on the impact to the business and the urgency for implementing the change.
- The Change Manager, Change Advisory Board, and other change stakeholders will ensure that segregation of duty controls are enforced during the building, testing and implementation of all changes.
- Access to alter the production environment is controlled, and access rights are only given to those people who are authorized to make changes.
- All changes require successful completion of testing before being implemented into the production environment.
- All changes to the production environment will be made within agreed change windows.
- Standard changes must be implemented using the accepted and established procedures, including obtaining approval from the delegated authority.
- Standard changes may be rescinded and reviewed at any time given unsuccessful results.
- Change Management metrics and management reports will be provided to management and Customers.
- Reviews are conducted by the Change Management Process Owner on a regular basis based on the process owner's discretion. Reviews will focus on the process consistency and repeatability and Key Performance Indicators (KPIs).

3.0 HOW TO BRING NEW/ADDITIONAL WORKLOAD TO DISA CSD

Business Estimate Process

1) **Initial Business Estimates (IBEs)[1] and Letter Estimates (LEs)**. While both IBEs and LEs rely on Customer requirements, IBEs do not require a significant level of detail to produce a price estimate, and typically will not have a full technical solution. LEs, on the other hand, are fully developed proposals that address complete Customer requirements. An IBE is an option for Customers and may be bypassed altogether in favor of an LE. Target completion timeline for an IBE is ten working days. The LE is the starting point for new workload, and therefore demands a greater amount of information, technical analysis, pricing and overall development of the document. Target completion timeline for an LE is approximately 30 working days.

2) **Process Steps**. By ensuring each step is addressed, the final outcome/product will be enhanced and will limit the risk of re-work and miscommunication of Customer expectations. It will also provide a stronger ability to implement efficiently in the event the estimate is accepted by the Customer. Furthermore, Customer Management representatives are encouraged to use existing templates and guides to help in the documentation of requirements, the development of IBEs and LEs, the pricing of services, and the review of final deliverables.

a) IBE
   i) First Contact: Initial communication between the Customer and DISA CSD. Outcomes include a tracking system entry, tracking number assignment, team/lead assignment, and delivery of service documentation (SLA, Service Catalog, and Terms and Conditions [T&C]) and forms (Service Request Form [SRF]) to the Customer.
   ii) Initial Requirement: Team lead works with the Customer to attain high-level system hosting requirements. Outcomes include a tracking system update, completed (high-level) SRF for IBE development & pricing, and determination (with CME) of ability to respond.
   iii) IBE Development & Pricing: As described above, the IBE is a method of delivering a quick price estimate to the Customer. The development of the document should restate high-level requirements, and the pricing should reflect general values related to A-goal and C-goal service prices. If an efficiency factor is applicable, a request must be made to CD1 for input. Outcomes include an IBE, Computing Services Customer Automated Price Estimator (CSCAPE) pricing entry, and a tracking system update.
   iv) CME or Division Review: Review details are discussed below. All IBEs will be reviewed at the CME-level or above prior to delivery to a Customer. At the division chief's discretion, the 48-hour Coordination step (see information below within LE steps) may be utilized. Outcomes include an approval or non-approval for delivery along with a tracking system update.

[1] The MHS Customer Branch will continue to use a pre-existing price quote routine and documentation with their Customers that does not include IBEs. However, the overall functionality of the IBE process remains in tact for them (i.e., Customer contact, requirements exchange, pricing, review, and delivery to the Customer for consideration). It is also not used as firm commitment by either party, but instead will lead to an LE if the requirement is valid.

v) Customer Delivery: Formal delivery shall consist of an email or other approved correspondence vehicle that will allow for a date, time and designated Customer to track progress. Outcomes include delivery to the Customer and a Collaboration and Process System (CAPS) update.

vi) Customer Acceptance: Customers wishing to accept or move forward from the IBE should be informed that an LE will now be developed, which will involve detailed requirements, a technical solution, implementation planning, and a more explicit price estimate. Outcome includes a CAPS update.

b) LE

i) First Contact: Initial communication between the Customer and DISA CSD (if the IBE path was not followed). Outcomes include CAPS entry, tracking number assignment, team/lead assignment, and delivery of the SRF to the Customer.

ii) Blue Team: Team lead works with the Customer to attain in-depth system hosting requirements, as well as address numerous issues including security posture, network/communication considerations, Customer's integrated milestone schedule, and funding availability. Outcomes include CAPS update, completed SRF for LE development & pricing, Bill of Materials (BOM) initiation, and determination (with CME) of ability to respond.

iii) Technical Solution: Team (including appropriate engineering, capacity, operations, communications, and other necessary representatives) develops a general plan for the implementation and management of the Customer workload. Outcomes include a technical solution, assumptions related to the solution, and a CAPS update.

iv) LE Development & Pricing: The development of the document should restate Customer expectations/mission, detailed requirements, assumptions, and the technical solution. The pricing should reflect the A-goal and C-goal service prices identified in the requirements and technical solution. Outcomes include an LE, CSCAPE pricing entry, and a CAPS update.

v) 48-Hour Coordination: To ensure that a formal proposal from DISA CSD represents an accurate description and pricing of our services, coordination with our service and financial management teams is required. The following list[2] shall be used for all LEs prior to CME Review or Customer Delivery:

(1) Availability Management Processor: Processor_Capacity_Review@csd.disa.mil
(2) Business Center: BusinessStrategyProposalReview@csd.disa.mil
(3) Storage: Storage_Engineer@csd.disa.mil
(4) Communication: CommunicationProposalReview@csd.disa.mil (pending)
(5) Facilities: Thomas.Mayberry@csd.disa.mil
(6) Labor: Gwendolyn.Stubbs@disa.mil and Marie.Wyrwa@disa.mil
(7) Technical Director: Ethel.Stewart@disa.mil and Reyes.Guerra@disa.mil

vi) CME or Division Review: Review details are discussed below. All LEs will be reviewed at the CME-level or above prior to delivery to a Customer. Outcomes include an approval or non-approval for delivery along with a CAPS update.

vii) Customer Delivery: Customers wishing to accept the LE should be informed that DISA CSD requires a formal approval (e.g., signed LE) and initial funding to include the implementation (one-time charges) and initial three months' operating (recurring) price. If initial funding is not available,

[2] The 48-Hour Coordination list will continuously change as DISA CSD personnel, groups, functionality and processes change. Please use this as a point-in-time list, with updates being done on a regular basis as needed.

the option of requesting a Commander's Order or another alternative should be reviewed at the CME-level or above.

3) **IBE & LE Review**.
   a) Division-Level Review ($5 M and up [annual value] or $1 M and up [implementation]). Applies to both IBEs and LEs at the specified value. Values incorporate all service, including labor, hardware, software, A-goal, C-goal, etc. Review will consist of validation of requirements, Customer goals, planning documentation, and overall coordination of events and milestones.

   b) CME-Level Review (Up to $5 M [annual value] or up to $1 M [implementation]). Applies to both IBEs and LEs at the specified value. Values incorporate all service, including labor, hardware, software, A-goal, C-goal, etc. Review will consist of validation of requirements, Customer goals, planning documentation, and overall coordination of events and milestones.

4) **Process Quality Improvement**. Semi-annually, the Customer Management Division will review the process and procedures, measure it against goals and expectations, and update this policy as necessary to better reflect steps needed to ensure efficiency. Anticipated dates include March and September.

5) **Tracking System**. Presently, the Customer Management Division has the CAPS at its disposal for tracking and reporting of our Customer business development process. We will continually review and revise this system to meet our needs until such time that another alternative is available.

6) **Metrics**. The Customer Management Division reports on the level of effort and timing related to the development of LEs. Given our Customers' interest in IBEs, we will begin to track their development as well to showcase the resources and timing associated with this output.

4.0 SERVER SIZING

The rate-based server billing methodology workload unit is the OE. An OE is defined as an instance of Operating System (OS) software. An OE can be a single server or a physical/logical server partition. The size of the OE is determined by the number of populated sockets being utilized. 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.)

All rate-based services (such as Basic, Hardware Services, etc.) are priced based on these sizes.

Windows/Linux OEs

- Mini OE - less than 1 socket per OE (only applies when virtualized OEs are being used)
- Small OE - 1 to 2 sockets per OE
- Large OE - greater than 2 sockets, up to and including 4 sockets per OE
- Enterprise OE - greater than 4 sockets per OE

UNIX OEs

- Small OE - up to and including 2 sockets per OE
- Medium OE - greater than 2 sockets, up to and including 4 sockets per OE
- Large OE - greater than 4 sockets, up to and including 8 sockets per OE
- Enterprise OE - greater than 8 sockets, up to and including 20 sockets per OE

5.0 HOST BASED SECURITY SYSTEM (HBSS)

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 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 Information Assurance/NetOps (PEO-IAN) 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-IAN has instituted support services that will enable the comprehensive implementation of the HBSS system 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 Information (formerly referred to as the INFOCON) plug-in module generates snapshots of asset configurations to facilitate detection of changes made to authorized baselines.
  - Rogue System Detection (RSD) is used to detect and react to unmanaged (or rogue) systems present on the network.
  - System Compliance Profiler (SCP) scans remote computers to determine whether they comply with policies. Access controlled by Public Key Infrastructure (PKI).
    - Self-service ~ Customer develops configuration from the Catalog of Services
    - Completed in one business day
    - Credit card or MIPR
    - $500 per month per server
  - Test and Development Environment
    - Install and test patches and upgrades
    - DISA STIG'd or PreSTIG'd operating systems
    - Development (compile or modify source code)

- CPU, memory, storage and OE provided
- Windows and Red Hat Linux environments available

- DISA DECC Hosting
  - Secure ~ network, physical
  - Reliable ~ data center environment
  - Dependable ~ 365/24/7 Help Desk support
- DECC-like Environment
  - DECC standard platforms and network infrastructure

6.0 HOW CAN GIG CONTENT DELIVERY SERVICE (GCDS) HELP YOU?

A great way to explain what GCDS can do for you is to ask: What challenges can GCDS solve in my organization?

If, as a Content Owner/Distributor, you:

- Need to serve globally distributed end users
- Have bandwidth challenged end users
- Have limited datacenter bandwidth
- Support mission critical applications
- Support a forward deployed user base
- Deliver large files (up to 1.8GBs)
- Need to scale quickly, or support unpredictable flash crowds
- Need to stand up web infrastructure quickly

Then the GCDS is the service you require.

The advantages and benefits of GCDS include:

Optimal performance

- Content and applications are served from locations near to the end users

Improved reliability

- No single point of failure
- Automatic failover

Massive scalability

- Global capacity on demand

Maximize resources

- No over-provisioning
- No redundant datacenters
- Simple to manage

Increased security

- SSL thru HTTPS
- Extending control to the edge of the network
- Defense in depth protects central infrastructure

Rapid implementation

- In a majority of cases, limited to Domain Name Service (DNS) changes with no software changes required

Edge enabling your web applications/portals on GCDS provides:

An enterprise solution leveraging Internet best practices

- Provides cost savings and economies of scale
- Can be leveraged by ALL services and combatant commands on the DISN

Faster web performance, leading to improved end user experience

- End users are mapped to the optimal GCDS server to retrieve cached content
- GCDS accelerates dynamic and non-cached content using various web application acceleration technologies such as compression, TCP optimization, persistent connections, pre-fetching, etc.

Enhanced security

- Integrates with existing authentication and authorization mechanisms such as SSL, client certificates, username/password
- Cloaks Origin Infrastructure. GCDS takes the first HTTP hit.

Increased availability and reliability

- Fault tolerant through multiple levels of redundancy and intelligent routing
- Provides intelligent and seamless failover for content owners

7.0 DISA CSD PARTNER PORTAL – WEB-BASED MANAGEMENT OF SLAS

DISA CSD has developed a web site, the Partner Portal, which is designed to be informative to parties both internal and external. It currently offers the following features:

A. Located as an extension of the internal CSD internal web, it is managed solely by CSD SLM personnel. There is no one between the Customers and CSD.

B. Provides web access to YOUR SLAs with CSD. All of our current SLAs are loaded in PDF and arranged by Service/Agency. They are linked to the Catalog of Services and the SLA T&C document so that the full range of information about our service offerings is immediately available. Another purpose is to actually manage the SLAs from this site. The SLA, with all modifications and all annual reviews, can be documented here. We are currently pursuing a Common Access Card (CAC)-enabled electronic signature capability which means SLAs can actually be "signed" on this site rather than faxing or mailing signature pages. Each Customer that has one or more SLAs with DISA will have view access to their SLAs. Initially, access is being established based on the POCs listed in the SLAs. These access rights can be changed at the Customer's request. All personnel within CSD that have a reason to see SLAs are also authorized view access. Also at the Customer's request, the Annual Financial Planning Estimates can be posted with their SLA.

C. SLA template and guidance. This is the standardized framework for all CSD SLAs along with the guidance necessary to build an SLA. A new rule for CSD SLAs is that they have an indefinite life and only require modification when the service offering mix is changed. Each SLA should be reviewed annually by both parties. This is also explained in the guidance.

D. The Partner Portal is home to the single, official, Catalog of Services and SLA T&C. By managing these two documents on this site, and using the SLA links to these documents, SLAs can be updated and kept current as rules and conditions change. If a modification to the catalog or T&C would materially change the way in which the service offerings are delivered, an SLA modification should be initiated by the CSD Account Manager (CAM) or CAR, who would ensure all Customers are made aware of those changes. All changes will be posted in the "Notifications" section of the Partner Portal.

E. A new Frequently Asked Questions (FAQs) section has been added that will include common questions that come to account managers, our Service Desks and from other sources of Customer interaction.

F. Access to both the production and financial portals for the Rapid Access Computing Environment (RACE).

G. Access to the DISA Worldwide Financial Network (DWFN) which is where electronic Customer invoices reside.

H. Access to Interactive Customer Evaluation (ICE) comment cards and Customer satisfaction surveys regarding your satisfaction with CSD's services and performance.

I. Other links, notes and announcements.

Any comments or questions about the Partner Portal or this Catalog of Services should be sent to:

DISASLA@csd.disa.mil

OR

DISA CSD SLA Hot Line
(303) 224-1660 (DSN 926)

OR

The CSD Service Level Manager
Mr. Mark Jones
303-224-1768 (DSN 926)
Mark.Jones@csd.disa.mil