Defense Information Systems Agency
Department of Defense

Defense Information Systems Agency
Global Information Grid (GIG)
Combat Support Directorate (CSD)
Center for Computing Services

TERMS AND CONDITIONS

APPLICABLE TO ALL SERVICE LEVEL AGREEMENTS (SLAs)

Published Date:

26 September 2008

Version 1.3

TABLE of CONTENTS

Service Level Agreement Terms and Conditions

Specific customer services, rates, and costs will be outlined in the Service Level Agreement (SLA), the Planning Estimate (PE), the Catalog of Services, and Terms and Conditions herein after referred as the Agreement.

1.0 GENERAL TERMS

a. Entire Agreement

The agreement is binding between DISA and the identified customers and collectively establishes the terms and conditions associated with the costs of all goods and services ordered and produced, in addition to reimbursement as a result of those customer orders. The purpose of the Agreement is to document the services that DISA CS shall furnish to the Customer. DISA CS shall deliver the services set forth in these documents. The Customer shall pay for the services covered by this Agreement in accordance with billing and payment terms incorporated in Section 3 of this document.

The provisions set forth in this Agreement, together with all modifications and amendments, constitute the entire agreement between the respective parties. Any verbal promises, representations, or understandings not expressly set forth in these documents are null and void. Any terms or provisions of the Agreement invalidated, void, or illegal shall in no way impair or invalidate any other terms or provisions herein, and the remaining terms and provisions shall remain in force. In the event either party reorganizes or merges with another organization, or otherwise operates under new organizational control, the Agreement shall apply to the succeeding organization(s) unless amended or terminated, in writing.

DISA CS agrees to provide processing and support services to the customer based on negotiated workload scheduling. Stated service levels, including timely delivery of products, will be achieved by the resources allocated to satisfy the customer projected workload and scheduled priorities. These service levels may be affected if there is a significant workload change or if the customer changes scheduled priorities without advance notice to DISA CS. Timely communication between DISA CS and the customer involving changes to agree upon priorities or workload are essential as such changes materially and financially impact both parties.

b. Modifications/Amendments/Renewals

(1) General

The SLA and the PE portions of this Agreement will be reviewed annually, or as required, to incorporate modifications or amendments to customer support requirements and to accurately reflect any changes or operational policy. Review and modification of the SLA will be made bilaterally, between DISA CS and the customer points of contact (POCs) with sufficient advance notification to permit appropriate resource adjustments.

(2) Modification

Modification refers to changes in word or form of the existing language contained in the SLA to accommodate changed requirements. This includes changes to workload requirements. Modification of the SLA may be requested by either party and must be in writing. Modification requires the approval and signature of both parties. An SLA modification should have sufficient lead-time to permit appropriate resource adjustments to be made.

(3) Amendment

Amendment refers to additive language incorporated into the SLA to accommodate additional and/or deleted requirements. Amendments to the SLA may be requested by either party and must be made in writing. Amendments must have approval and signature of both DISA CS and the customer.

(4) Renewal

The customer and DISA CS shall review the SLA and PE annually, or as required, to determine if modifications or amendments are needed to reflect the customer's support requirements for the next fiscal year. Modification/renewal documents require the approval and signature of both parties.

(5) Procedures for Modification, Amendment, or Renewal

Negotiations shall be between DISA CS and customer POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA shall remain in effect. DISA CS and the customer anticipate that once signed, the terms and provisions of the SLA remain in effect until jointly modified by the customer and DISA CS, or until terminated by either party. Annual reviews will identify required changes, resulting in an updated SLA and corresponding PE, recording and representing the SLA renewal activities.

2.0 DURATION of AGREEMENT

The SLA is reviewed annually, at a minimum, or as required, ensuring DISA CS is furnishing all the negotiated IT services required by the customer. The annual review provides a forum for the customer to identify future workload requirements. Annual reviews will identify required changes, resulting in an updated SLA and corresponding PE, recording and representing the SLA renewal activities.

3.0 PRICING and PAYMENTS

a. Payment

The Service Level Agreement between DISA Computing Services and a Customer will have an indefinite life. The SLA is a description of services and service levels that DISA Computing Services shall provide. It will be reviewed annually to ensure that the services included are still accurately described. Additionally, when a Customer agrees to new/additional workload support from DISA Computing Services via acceptance of a Letter Estimate (LE), the SLA will be amended to include the new work and the related Planning Estimate (PE) (or new PE) will be adjusted by the agreed upon price.

During the fiscal year 3rd quarter the customer will receive an updated PE for the next fiscal year. If the SLA still provides an accurate accounting of services and support to be delivered, and the PE represents a reasonable estimate of the anticipated workload and the related costs, the Customer should accept and sign the PE. DISA Computing Services is subject to the financial rules applicable to a Defense Working Capital Fund (DWCF) business entity, Customer funding must be received prior to any provision of service.

(1) DoD customers

Upon agreement of a SLA, an appropriate Customer representative is required to sign the SLA as is the DISA Computing Services Customer Management Executive (CME). Upon signature of the SLA, DISA Computing Services becomes obligated to provide the services described in the SLA, as amplified by this Terms and Conditions document and the Catalog of Services. The Customer shall be obligated to meet the Customer requirements included in this Terms and Conditions document. The SLA does not require annual renewal and signature, but will be managed as described in the previous paragraphs.

Upon signature of the PE, the customer becomes obligated to pay DISA CS for services delivered in accordance with the SLA at the prices identified in the PE. PE’s are renewed annually and must be signed by DISA Computing Services and Customer personnel annually. The customer shall submit all Military Interdepartmental Purchase Requests (MIPRs), DD Form 448, to the DISA Financial Management Liaison Office (FMLO) in Pensacola, FL, prior to delivery of any services. The MIPR shall provide funding to cover estimated charges for at least one quarter, with amendments executed prior to the start of each succeeding quarter. At the beginning of the fiscal year, funding may be provided contingent on passage of a Continuing Resolution or DoD Appropriations Act, whichever is applicable. The FMLO office shall submit a MIPR Acceptance Form (DD Form 448-2), to the customer, that acknowledges acceptance of the funds received.

(2) Non-DoD customers

It is normally not the practice of DISA Computing Services to provide support to non-DoD agencies and other entities. However, under certain conditions it may be deemed appropriate to provide such support. When it is decided that such support will be provided, the rules discussed herein regarding SLA’s and PEs will be applied. It is understood that some revisions may be required, such as the method of payment. When such revision is required, the agreed upon methods will be included in the SLA.

4.0 REQUIREMENTS OF ORDERS FOR WORK TO BE PERFORMED

As a general rule no work or service shall be performed by DISA CS except on the basis of reimbursable orders, received and accepted, that constitute obligations of Federal Government ordering activities or advances from non Federal Government entities as directed by DoD Financial Management Regulation 7000.14-R, Volume 11B. Work for customers may begin in advance of receipt and acceptance of a formal order under two circumstances, as follows:

(1) Letter of Intent Orders. When it is desirable, in the interest of economical operations, to incur limited costs in advance of the receipt of a regular order for an authorized program for which customer funds are available, such work or services may be undertaken on the basis of a letter of intent. This letter constitutes an obligation of the ordering activity in a stated amount sufficient to cover the advance costs that may be incurred.

(2) Commanding Officer’s Orders. When it is necessary to begin work of an emergency nature prior to the receipt of an order, a commanding officer/director’s order or similar order may be issued by the Director, DISA CS, subject to the following conditions:

(a) DISA CS must have written assurance that an order shall be issued promptly or shall have equivalent documented communication. The use of such orders should be limited to situations in which there are bona fide emergencies arising from unforeseen urgent requirements;

(b) A director’s order shall expire within 30 days from the date of issuance;

(c) A director’s order shall be issued on a local form and shall be approved and signed by the director or an authorized representative.

This regulation applies under the conditions of a continuing resolution.

5.0 FUNDING DOCUMENTS

Funding documents shall be addressed to the DISA CS Funding Document POC in accordance with the POC listing of the SLA. In addition to the dollar amount, the funding document shall contain (in Block 9 of the MIPR) the name and telephone number of the customer's POC, the customer's Unit Identification Code (UIC), DoD Activity Address Code (DoDAAC), the Billing Account Number (BAN), and the SLA Number assigned by DISA CS. Where practicable, Block 9 shall identify the application and/or the Application System Code (ASC).

6.0 INVOICING AND BILLING

Routine invoicing will commence at the beginning of each fiscal year to reflect services provided regardless of SLA/PE signature status. All customers may view invoices detailing IT services performed/received online at (insert DWFN link here) in the DISA CS Centralized Invoice System (CIS). Current month and year-to-date invoice data will be updated monthly, reporting actual charges incurred. The customer shall work with DISA CS to ensure that the appropriate Invoice Account Code (IAC) and ASC are assigned to allow accurate capturing of the customer's usage data at the required level.

The customer will be billed immediately via cross-disbursing procedures. The customer shall promptly review the bill and invoice, notify DISA CS of any disputed billings, and otherwise expedite certification of the bill. Subsequent customer billings will include any adjustments arising from disputed billings.

7.0 BUSINESS MANAGEMENT MODERNIZATION PROGRAM (BMMP)

The customer must provide the required documentation specified in the FAQs Certification Approval guide. Such documentation must be provided as part of the customers acceptance of this offering before implementation can proceed.

8.0 BILL PAYER CHANGES

If the bill payer changes, the funding responsibility for an existing workload remains with the originating bill payer until the FMLO office receives written notification of the new bill payer, the effective date, and a MIPR from the new bill payer. DISA CS and the FMLO office should receive this data at least 30 business days prior to the effective date. DISA CS will change the appropriate Customer Identification Code (CIC) upon receipt of the new information.

9.0 DISPUTE RESOLUTION

On April 13, 2007, OUSD Comptroller directed all Components to establish supplementary procedures to ensure the department is in compliance with Treasury Financial Manual, Bulletin No. 2007-03 by October 1, 2007. An alternative Dispute Resolution clause is as follows:

1. Disputes resolution shall involve, the program offices, resource management office, the accounting offices, the contracting officer, and the agency's Chief Financial Officer (CFO), as

appropriate. Disputes shall be documented in writing with clear reasons for the dispute. A memorandum of agreement will be signed by the CFOs of each department and agency to acknowledge that department's or agencies active participation in the dispute resolution process.

2. Trading Partners shall not chargeback or reject transactions that comply with these Rules. Further, new transactions shall not be created to circumvent these Rules. Transactions that comply with these Rules, but are disputed, shall be resolved as delineated in paragraph below. Disputes are of two types: accounting treatment (e.g., of advances, nonexpenditure transfers) and contractual (e.g., payment, collection, interagency agreement).

   a. If intragovernmental differences result from differing accounting treatment, the Trading Partners have 60 calendar days from the date that (1) the difference is identified in the Material Differences Report (Attachment 2), or (2) a charge is disputed, whichever comes first, to agree on the treatment of an accounting entry. If agreement cannot be reached, both Trading Partners' CFOs shall request that a final decision be rendered by the CFOs Council's Intragovernmental Dispute Resolution.

   b. If intragovernmental differences result from contractual disputes, the Trading Partners have 60 calendar days from the date that (1) the difference is identified in the Material Difference Report, or (2) a charge is disputed, whichever comes first, to agree on the contractual terms. If agreement cannot be reached, both Trading Partners' CFOs shall request that a binding decision be rendered by the CFOs Council's Committee established for this purpose. The Committee shall render a decision within 90 calendar days of request. The Trading Partners will then coordinate to ensure any necessary IPAC transaction needed to effect the decision is processed as applicable.

   c. Missing indicative data on an intragovernmental transaction (as delineated in paragraph III.D.2) is cause for a contractual dispute. The Buyer may establish a monetary threshold before asking for contractual decisions; the threshold shall not exceed $100,000 per order. If an amount is under the Buyer's threshold, and the Buyer elects not to pursue a dispute, then the Buyer shall pay the amount.

10.0 TERMINATION of AGREEMENT

Termination will be conducted in accordance with guidance provided in DoDI 4000.19 requiring 180 days termination notification. Termination charges will be negotiated and charged on a case-by-case basis. With the proper coordination, the termination of an application can occur within 60 days.

With assistance of the DISA CS Customer Account Representative (CAR), the customer will provide a completed Agreement Termination Worksheet provided in Appendix A.

11.0 MANAGEMENT AND CONTROLS

a. Applicable regulatory guidance

DISA complies with all regulatory guidance issued by DoD, a list of relevant documents, with links, in provided to Section 6 of the Catalog of Services.

DISA complies with the recommended security controls for federal information systems as specified in the NIST Special Publication 800-53.

b. Management Process

The customer shall provide estimates of anticipated workloads with which DISA CS can develop a target budget amount for the PE. DISA CS will provide workload history, where it is available, to aid in this estimate.

(1) Workload Estimates: DISA CS will provide the customer with actual mainframe and storage usage information, server, and server storage usage capacity analysis being provided during the year. To develop meaningful projections, the customer and DISA CS should collaborate, as the customer is ultimately responsible for all mainframe and server projections.

(2) Budget Estimates: The customer uses workload estimate information to submit a budget estimate for funding. If a difference between the customer budget submission and final approved appropriation exists, DISA CS, in conjunction with the customer, shall adjust the services in the SLA accordingly, matching services to the customer funding level.

(3) SLA Preparation: The SLA must be specific as to the types and levels of services required. The customer must furnish the projected workload for DISA CS to effect the proper level of support. The Terms and Conditions document contains provisions that apply to all customers and to most business relationships. The SLA contains additional customer requirements that are consistent with the Catalog of Services, and required appendices to identify unique requirements.

12.0 SYSTEM TECHNOLOGY

a. System Architecture

The IA architecture is defined to meet, at a minimum, the service requirement for the MAC II, Sensitive, Medium Robustness, system configuration, network configuration and customer support requirement identified in the NIST Special Pub 800.53 and DoD directive 8500.2.

(1) Server

The standard Server Enterprise Architecture (SEA) is a set of minimum requirements in order for a server to be placed in a DISA CS environment. These standards were developed by taking into account best practices, network requirements, storage requirements and overall general knowledge of the DECC environment. The Strategic Engineering Division of Computing Services under the direction of the Technical Director created these standards.

(2) Storage

The Storage Line of Business (Storage LOB) Storage Enterprise Architecture (SEA) is based upon the DoD Joint Technical Architectural (JTA) Framework Version 4.0. The DoD JTA Framework was developed in accordance with the General Auditing Office (GAO) Enterprise Architecture Management Maturity Framework published in February 2002. The Storage LOB modified this framework, as deemed appropriate for the DISA CS Fee-for-Service computer center operations

b. Current Configuration

(1) Server

There are currently two core hardware server platforms in Computing Services; RISC Based servers from Sun, HP, Fujitsu and IBM, and x86 based servers from multiple vendors such as DELL, IBM and HP. The capacity services contract, managed by the Processor Line of Business (PLOB), will provide hardware and operating systems that will eventually replace the current hardware with HP for HP-UX and x86 servers, IBM for the AIX platform and SUN for Solaris. The Processor LOB can provide details of these servers.

(2) Storage

(a) Disk and magnetic tape technologies are the major data storage technologies used to support all operating systems.

(b) Disk is used to hold databases, data warehouses, and flat files where immediate access to the data is necessary.

(c) Magnetic tape is used for backups, archives, and for those files that do not need to be immediately accessed.

In the mainframe environment storage devices are often shared physically and/or logically between processing platforms while the server environment primarily relies upon dedicated storage resources at the operating system level.

Fibre channel (FC) Storage Attached Network (SAN) is the primary solution provided. However, in special cases, with associated documentation, DISA can deploy Direct Attached Storage (DAS) and Network Attached Storage (NAS) solutions. A variety of backup configurations are possible included Disk-to-Disk and replication.

Note – Corporate direction is to base all workload in a SAN-connected arrangement.

DISA CS employs automatic tape libraries to support the data backup and archiving process. DISA has an off-site tape storage contract for safe and efficient tape storage. Symantec (Veritas) is the software used for backup.

Note – Corporate direction is to eliminate manual tape management processes, supporting workload efficiencies related to time management, economies of scale and technology / process standardization.

c. Changes in Technology

(1) Server

The largest change coming to CS will be the extensive use of server virtualization technology. In the Intel™ space this will be accomplished with VMWare Virtual Infrastructure. VMWare has a myriad of capabilities such as VMotion (moving a running virtual machine (VM) from one physical server to another with zero downtime), DRS (Dynamic Resource Scheduling) which is the capability to place up to 16 physical servers in to a resource pool where workloads can utilize resources on the fly and High Availability (HA) which allows a VM to be started on another physical host automatically in the case of a hardware failure.

In the UNIX space virtualization comes in multiple flavors and each vendor does partitioning slightly different but the following are basic descriptions. Physical or hard partitioning is defined as subdividing a single server, such that all power, CPU, memory and I/O devices used by a partition are dedicated to that partition and no other. A physical partition will have the following characteristics:

(a) Dedicated power. Power can be shut off to the partition without impacting any other partition

(b) CPU and memory are allocated to the partition based on hardware configuration, and cannot be shared with another partition, or be dynamically reallocated.

(c) All I/O devices are dedicated to the physical partition including Ethernet cards, HBAs, disk drives, and optical drives.

(d) May be configured as a single OS, or host multiple virtual OS's

Virtual or Soft Partitions may have some attributes of physical partitioning, but not all, depending on the server and OS manufacturers. Generally you may have multiple virtual partitions within a server, or within a Physical partition. Resources (CPUs, Memory and I/O) can be shared between the virtual partitions, either dynamically by the operator, or during boot-up configuration.

Click this link to see the CSD Standard Architecture briefing.

(2) Storage

The foundation of the architecture is a high-speed Core/Edge SAN consisting of fibre channel switches and directors connecting IBM mainframes and servers to their storage devices - disk, optical and tape (traditional and virtual) at each processing location. The SAN provides all standard storage functionality such as mirroring, data replication, data snapshots and security protection. The SAN supports all platforms at the processing location. The SAN expands or shrinks to meet changing requirements. Storage Devices on the SAN will be low cost and highly reliable. Each device can support all operating system environments on the SAN. Assured computing techniques are designed into every SAN. A SAN will exist at each processing location but some may be managed remotely from a Systems Management Center (SMC).

The SAN provides over 75% of the storage required by CS customers.

(a) Open Systems – Diskless servers will become the dominant server architecture in the new environment. Exceptions are allowed for specific reasons such as satisfying extraordinary customer requirements; however, if DISA CS must manage the server-based storage devices / amounts, then those storage amounts, as measured in allocated raw gigabytes, will be included in the Storage Billing Rate calculations.

(b) Mainframe – The IBM mainframe environment uses the same storage technology as the servers; however IBM mainframe storage is still managed separately pending the development and maturing of Storage Resource Management (SRM) technology that is able to manage both server and IBM mainframe storage assets from a single application.

13.0 SECURITY AND ACCESS

a. Security Measures and Procedures

Security mechanisms shall provide the appropriate level of information assurance controls based on the Mission Assurance Category (MAC) and Confidentiality Level to ensure the correct level of assurance for the confidentiality, integrity, and availability of data entrusted to DISA CS for processing and storage under the SLA. DISA CS utilizes the DoD Instruction 8500.2 and all other established DoD guidelines for ensuring adequate controls are in place to safeguard the data entrusted to it based on the MAC level, Confidentiality Level, and robustness as specified by the customer.

DISA CSD and the customer recognize that providing for the availability, authentication, confidentiality, integrity, and non-repudiation of information stored, processed, and transmitted is a shared responsibility. It is understood, data sharing/manipulation across customer applications is strictly prohibited and destruction of data is in accordance with DISA CSD local policy and procedures.

DISA supports the Federal Information Security Management Act (FISMA) that was passed by Congress and signed into law, it is part of the E-Government Act of 2002 (Pub. L. No. 107-347). http://iase.disa.mil/fisma/index.html

(Requires input from security personnel for necessary steps to complete if C/A, not finalized as stated in the SLA)

14.0 OWNERSHIP and LICENSES

a. Data

As the service provider, DISA CS is required to certify and accredit the platforms/systems operating in the computing centers. Customers operating applications on the systems within the computing centers are required to certify and accredit the applications as the owners of the data processed/produced in these applications.

b. Hardware

It is preferred that DISA CS acquire, own and maintain all hardware supporting customer workloads. DISA has negotiated a series of indefinite-delivery; indefinite-quantity capacity services contracts to obtain Unisys and IBM Mainframes and Windows, Linux, and Unix Servers. DISA has a variety of contract vehicles to acquire the hardware to meet customer needs.

DISA requires the below standard level of maintenance support for all assets owned and/or maintained by DISA CS.

Storage	24 hours x 7 days x 4 hour response
Server	24 hours x 7 days x 4 hour response
Mainframe	24 hours x 7 days x 2 hour response

Maintenance support levels other than the above may be negotiated if required, and annotated in the SLA.

(1) Customer-Owned Hardware Assets: It is preferred that DISA CS acquire, own and maintain all hardware supporting customer workloads. Customer owned/customer maintained hardware assets hosted at DISA CS facilities will not be maintained or supported by DISA CS.

If the customer is proposing to provide their own hardware, two options are available.

(a) Customer Owned / DISA CS Maintained

If the customer desires that DISA CS maintain their hardware, the following items are required:

1. Completed Customer Owned Hardware Form located in Appendix B must be submitted to DISA CS within thirty (30) days of anticipated customer processing start date or within thirty (30) days after any change of equipment. A copy of the Hardware Form is located in Appendix B.

2. To ensure that DISA CS can provide appropriate, uninterrupted maintenance support to the customer owned asset(s), the customer should ensure that the warranty acquired with any hardware meets the minimum maintenance requirements stated above.

(b) Customer Owned Hardware Transfer

If DISA CS is to take over maintenance responsibilities for customer owned hardware, the following items are required:

1. Completed Customer Owned Hardware Form located in Appendix B must be submitted to DISA CS within thirty (30) calendar days of anticipated customer processing start date or within thirty (30) days after any change of equipment.

2. To ensure that DISA CS can provide appropriate, uninterrupted maintenance support to the customer owned asset(s), the customer should ensure that the warranty acquired with any hardware meets the minimum maintenance requirements stated above.

c. Software

(1) Standard Operating Environment

DISA CS establishes and enforces a comprehensive, standardized enterprise software suite in order to increase efficiency, improve performance, and ensure perpetual processing capability.

Standardization of software products reduces the number of functionally equivalent products in the inventory, lowers software maintenance, licensing, and operating costs, and creates a seamless environment under which customer applications can operate.

The Standard Operating Environment (SOE) is comprised of a three-tiered architecture:

Base Operating System
Includes the native operating system, as well as other operating system services, including the management of the hardware processes, memory, devices, signals, and clock system. This level includes the Operating Systems Services.
Core Services
Includes services to manage the internal flow of data within the system, control communication with other platforms, and manage system resources. This level includes the Distributed Systems Services, Network Services, Print Management Services, Security and Audit Services, Storage Management Services, System Administration Services, System Support Monitor Services and System Utilities.
Application Services
Includes services that support the development, maintenance and execution of applications across the enterprise. This level includes the Applications, Application Development Tools, Data Access Services, Data Management Services, General Utilities, Language Services, Open Services, Report Managers and Transaction Processing Monitors.

(2) Executive Software

“Executive Software encompasses the Front End Processor (FEP) or premise router back to the computer system itself (mainframe, mid-tier).”

For purposes of DISA CS software management, the scope of executive software has been defined to be:

The basic operating system, utilities, tools and other COTS and Government Off the Shelf (GOTS) software products used to control and manage the execution of functional applications and their interaction with the hardware configuration. Executive software allows the processing of specified data against an application to produce the intended results.

Click this link to obtain a current and complete listing of the SOE software.

Select SOE plotter.xls from the SOE selected Product Matrix box(located in Documents box).

(a) Executive Software Management
Executive software operating in a Computing Services environment is licensed to DISA CS. DISA CS will perform installation, maintenance, and technical support for DISA CS owned standard Executive software packages. DISA CS will maintain the most current software version, licensing documentation, and release levels acquired under existing contract maintenance terms. DISA CS will apply service packs, hotfixes, security releases and other patches as appropriate. Activities related to the sustainment of Executive software will be coordinated with the customer and users.

DISA CS can only support customer required executive software when ownership of this software is transferred to DISA CS. If the customer is proposing to provide their own software, with transfer of these licenses, the transfer will need to be negotiated with DISA CS in advance.

(3) Application Software

(a) IBM Mainframe
All software supporting a customer application must be licensed to DISA CS. No software is permitted to operate on the mainframe that is not DISA CS owned. DISA CS will procure necessary software on behalf of the customer and charge the customer accordingly.

In FY07 and FY08 DISA CS will begin removing mainframe software products in the Application Services layer of the SOE Model from the mainframe rates such as Report Distribution tools (CA DISPATCH, Control D), Report Writing tools (Crystal Reports, Cognos), etc. In FY09 software products removed from the rates will be directly charged to the customer. Database Management System software and Database software utilities are already charged to the customer directly.

Customers are encouraged to standardize application software across their organization to minimize the number of software products directly charged to them. For mainframe applications, a product selected by a customer as an organizational enterprise standard (removing all functionally redundant software throughout the Service/Agency) will be included in the mainframe rates. The DISA CS enterprise asset management tool will be utilized to 'attach' application software products to customer applications using the ASC. To avoid paying direct charges for products at the Application Services layer, all functionally redundant products must be removed within 18 months following the standard software product selection. If, after a software product has been selected as a standard for a customer's organization, a new functionally redundant software product is requested for installation, the previously selected software product will be removed from the mainframe rate and that product and the new functionally redundant software product will be charged to the customer directly. Customers will also be charged Single Version Charges (SVC) for versions of software that vendors have discontinued support for but are still being used in a customer's application.

(b) Server

In FY07, the Server LOB established a server rate to include the software license maintenance costs for the Oracle database. With the exception of this software product, all server software in the Application Services layer of the SOE model is directly charged to the customer.

The preferred method is for DISA CS to acquire, own and maintain all software operating on servers for DISA to ensure that appropriate, uninterrupted maintenance support is provided.

(c) Unisys

Unisys software product charging methodology remains unchanged.

(4) Software Transfers

The preferred method is for DISA CS to acquire, own and maintain all software. To provide the best possible support to the customer, it is recommended that customer owned software be transferred to DISA CS.

(a) Mainframe

Mainframe software is not generally transferable unless approved by the software vendor. All software operating on mainframes must be licensed to DISA CS.

(b) Server

Server software is generally transferable without vendor approval. It is the responsibility of the current owner to provide proof of ownership and to assure that licenses are transferable.

If the customer is proposing to provide their own software, the following guidelines are required by DISA CS, to ensure that appropriate, uninterrupted maintenance support is provided to customer owned software. The following items are required in order to effect the transfer:

1. Signed Software Transfer Agreement submitted to DISA CS. A copy of the Transfer Agreement is located in Appendix C.

2. The data elements table must be completed in its entirety for each software license/maintenance agreement being transferred.

The completed Software Transfer Agreement should be forwarded to:

DISA Computing Services – Logistics
ATTN: GS433 (Customer Support)
1 Overcash Avenue
Chambersburg, PA 17201-4123

3. For software currently covered under a renewable maintenance contract, please notify the appropriate vendor(s) to change the address for renewal notification to:

DISA Computing Services – Logistics
ATTN: GS431 (Software Maintenance)
1 Overcash Avenue
Chambersburg, PA 17201-4123

4. Originals or copies of all documentation that establishes/demonstrates proof of ownership for the software to be transferred. Certificates of Ownership/Origin, vendor-accepted contracts or delivery orders, purchase invoices, and/or maintenance renewal invoices are acceptable proofs of ownership.

5. Any media containing original or backup copies of the software, which could be of use to DISA CS.

15.0 DISA RESPONSIBILITIES

DISA CS is responsible for the security of all DISA CS owned and controlled technical environments that supply services (i.e. during transport, processing, and storage on DISA CS' platforms and servicing networks). Based on applicable DoD guidance and the NIST Special Publication 800-53, DISA CS will certify to the customer that the required security mechanisms are present and operational.

a. Respond to any in-cycle changes to workload estimates or support requirements after formal notification of such changes by the customer.

b. Respond to customer requests for exceptions to normal processing within 10 calendar days after formal notification.

c. Ensure that the customer has access to their data. Provide end-to-end encryption through the Mainframe Internet Access Portal (MIAP) that furnishes DoD with the ability to authenticate commercial Internet users to gain access to the DoD networks.

d. Furnish to the customer a primary and an alternate DISA CS POC and update these as necessary.

e. Notify the customer of:

(1) Changes to established hours of processing or service availability;

(2) Scheduled downtimes or other restrictions to processing or service availability, at least 72 hours in advance;

(3) Hardware and software upgrades, releases, and changes which may impact the customer; and

(4) Any suspected or known security deviations or violations.

f. Negotiate a BCP with the customer.

g. Implement an acceptable Risk Management Plan in order to certify and accredit, or recertify or reaccredit DISA CS (facility, environment, operating systems, supporting utility software to operating systems, and network infrastructure) in accordance with DoDD 8500.1 and DoDI 8500.2. DISA CS is required to provide protection for information processed by the operating systems within the DISA CS/customer agreed MAC Level in accordance with DoDD 8500.1 and DoDI 8500.2.

h. Establish and maintain a Personnel and Information Security Program to ensure access is in accordance with applicable DoD security directives.

i. Establish a system for managing access control to the operating system and its supporting utility software.

j. Furnish all notifications and information to the customer in writing via memorandum or electronic mail; and by telephone, if urgent, to confirm receipt.

k. Meet with customer representative(s) as required by the customer, to discuss DISA CS performance, issues, areas of concern, anticipated workload changes, and any changes or modifications to the Agreement or BCP.

l. Install executive software upgrades, normally once per year.

16.0 CUSTOMER RESPONSIBILITIES

The customer is responsible for ensuring control of all data retrieved from within DISA CS technical environments, and for the security of any and all customer owned and controlled technical environments. The customer will provide certifications to DISA CS that their security mechanisms are present and operational. In addition to the specific customer responsibilities set forth elsewhere in this agreement, the customer will perform the following:

a. Develop applications that will interface and exchange identification and authentication with the known security products utilized by DISA CS and the DoD sanctioned Security Technical Implementation Guides (STIGs) and Application Information Assurance Controls in accordance with DoDI 8500.2.

b. Certify and accredit the customer security infrastructure (hardware, operating system, and internal communications) in accordance with DoDI 5200.40, DoD Information Technology Certification and Accreditation Process (DITSCAP) and DoDI 8510.1-M, DITSCAP Application.

c. Any specialized or additional communications support requirements by the customer must be submitted 120 days in advance for Automated System Interruption (ASI) and seven to ten days for general requirements. Urgent requirements will be handled on a case-by-case basis. All ASI requests must be submitted to the supporting OST.

d. Provide the following general IA information for their AIS and notification of any changes in writing to DISA CS:

(1) Provide the MAC and Confidentiality Level (CL) for their applications;

(2) Ports, Protocols, and Services that their AIS utilizes for outbound and inbound routing into the wide-area networks;

(3) Identify any required DoDI 8500.2 IA controls based on the MAC and Confidentiality level that have not been implemented

(4) Identify any known risk that has been accepted by their Designated Approving Authority (DAA);

(5) Approving authorities for access. Include name, telephone number and e-mail address. DISA CS restricts adding users to the application, in the absence of this information;

(6) Provide classification guidance for applications handling classified information.

e. Immediately direct any security incidents through customer security channels and DISA CS (if affected by the incident).

f. The customer Program Manager (PM) is responsible for following Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01. They must monitor and respond to Information Assurance Vulnerability Alerts (IAVAs) and provide DISA CS with a software release or mitigation plan. The PM should monitor OS and application security patches from the vendor and provide releases to DISA CS. Security patches from the vendor should be no more than one (1) generation old.

g. Those customers, who are given the authority to add, delete, change, and unlock locked system accounts, agree to maintain a copy of the DD Form 2875 for each active user. They also agree to provide a copy of the DD Form 2875 upon request to Computing Services.

h. The Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2005 states that funds appropriated to the DoD may not be obligated for a defense business system modernization that will have a total cost in excess of $1M unless: a. the approval authority designated for the defense business system certifies to the Defense Business Systems Management Committee (DBSMC) that the business system modernization is in compliance with the enterprise architecture; and b. the certification by the approval authority is approved by the DBSMC.

A defense business system modernization is the acquisition or development of a new defense business system; or any significant modification or enhancement of existing defense business systems (other than necessary to maintain current services). (10 U.S.C. 2222 (j) (3)). The customer is responsible to submit a copy of the OSD DBSMC certification results or certification control number for the proposed business system, prior to DISA CS obligating funding for services. Failure to present the appropriate documentation precludes DISA CS from taking further action or providing services until the time documentation is submitted.

i. Furnish DISA CS with projections of future workload levels and support requirements at the Customer Identification Code (CIC) and the Application System Code (ASC) levels. These should reflect known or anticipated changes not less than 180 calendar days prior to the known change.

j. Notify DISA CS of in-cycle changes to workload estimates or support requirements, as they become known.

k. Pay DISA CS for appropriate operational support costs if the customer retains ownership of any equipment, and if DISA CS furnishes that support. The customer will maintain/replace/upgrade the equipment, as required, to run the customer's applications.

l. Coordinate with DISA CS on any exceptions to normal processing as soon as they become known. Normal processing services are specified in the SA and Exceptions to Normal Processing are defined in the Glossary.

m. Furnish both the primary and alternate customer POCs to the DISA CS OST, and update as necessary. In the event the OST cannot contact the primary POC, the alternate on the list will be contacted. The customer POC will notify the customer users of any operational situations that impact service.

n. Work with the appropriate DISA CS representative to prioritize their applications and to develop their BCP.

o. Maintain access control for users to their applications.

p. Provide written identification of all Controlled Unclassified Information applications and information being processed for them by the DECC(s), and the required protection during transmission.

q. Furnish all notifications and information to DISA CS via memorandum or electronic mail; and by telephone, if urgent, to confirm receipt.

r. Make appropriate modifications to applications in support of periodic executive software and hardware upgrades.

s. In order to facilitate recovery of network data communications, customer applications referring to hard-coded Internet Protocol (IP) addresses must be changed to Domain Name Server (DNS) addresses where possible. In the event of severe service interruptions or disasters, this will allow nodes to be switched to alternate nodes with minimal impact to customer data communications.

17.0 HOW to BRING NEW or ADDITIONAL WORKLOAD to DISA CS

Initial contact will be with the assigned Customer Management Executive (CME) for your organization. The CME team will coordinate the completion of the Service Request Form (SRF) specifying your requirements. Following the completion of the SRF, the requirement will have costs applied and returned to you in a Letter Estimate. Upon your affordability/feasibility assessment and acceptance by your organization, within 60 days, a detailed implementation plan will be developed with execution timelines.

If we do not have an existing relationship with you, please submit your request to DISA CS Customer Management Division DISA_ComputingServices_CustomerHotline@den.disa.mil or 303-676-1660.

Initiation of Billing for New Workload

Initiation of Billing occurs in 2 Steps commencing at Initial Functional Capability (IFC)

Step 1

Includes One Time costs associated with implementation

Step 2

Initiation of annual sustainment costs.

Note: Initial Function Control (IFC) is not necessarily synonymous with Initial Operational Capability (IOC). To achieve IOC, all items identified in the IOC Checklist provided in Appendix D are required.

APPENDIX A. - TERMINATION WORKSHEET

DISA Center for Computing Services Termination Worksheet	
Customer Name:	
Email:	
1. Data System Designator (DSD) if applicable:	
2. If this covers only a partial DSD please explain:	
3. System Name:	
4. System Location:	
5. Shutdown date by site: (This date will deactivate processing capabilities. The system will be idled, but data will be kept intact and the ability to bring back online as a backup or fail measure is still an option. Storage of these files will incur machine utilizations costs until final shutdown. If needed, additional dates and sites can be provided).	
6. Final Decommission date by site: (This is the date that officially shuts down all files and storage capability unless specific arrangements are requested in item 12).	
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
7. Replacement Automated Information System (AIS) if any:	
8. Replacement System Name:	
9. Interfacing System/s and impact:	
System(s):	**Impact(s):**
System(s):	**Impact(s):**
System(s):	**Impact(s):**
System(s):	**Impact(s):**
System(s):	**Impact(s):**
10. Coordinating System POC: (name and phone number)	
11. Date Coordinating System POC notified:	
12. High Level Qualifiers for data deletion: (This input mandatory for IBM- Minimum of two. Identify as applicable)	
12a. IBM Accounts:	
12b. Unisys Accounts:	
12c. Server Accounts:	

Archiving Files Special Instructions	
13. Do you want to delete or archive datasets?	
14. High Level Qualifiers used for archiving:	
15. Organization to perform the archive:	
16. Organization to maintain the archive:	
17. Identify bill payer and Billing Account Number (BAN)	
18. Identify production jobs to be removed from the schedule:	
19. Identify any software unique to this DSD that is no longer needed.	
20. Identify other billable items for which service is no longer required such as CA Dispatch prints, special reports etc:	
21. Identify retention requirements with media and data set name if different than listed in item 14 above.	
22. Shipping address where archived files are to be sent/returned for storage.	
Authorization Signatures:	
23. Functional Owner	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	
24. Customer Management Division	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	
25. Resource Management Division	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	

26. Operations Division	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	
27 (Other – as required)	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	
28. (Other – as required)	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature	
Any questions regarding this form can be directed to Customer Management Executive POC: DSN:	

APPENDIX B. - CUSTOMER OWNED HARDWARE FORM

DATA ELEMENT	ASSET DESCRIPTION
Manufacturer Name	
Model Number	
Serial Number (as printed on the nomenclature plate)	
Bar Code (if available)	
Device/Class ID (i.e. Mainframe CPU Complex, Mid-tier Server, Mainframe Controller, Mid-tier Robotic Storage, Mainframe Cartridge Tape Drive)	
Contract/Warranty Number (existing maintenance contract)	
Expiration Date (date maintenance contract or warranty expires)	
Vendor Help desk Phone Number (The contact number of the vendor to call in the event of maintenance service) DISA Helpdesks will contact this number to initiate a service call.	
Customer POC (Name of Government personnel to call in the event of problems with the service call).	
Acquisition contract number	
Acquisition date	
Acquisition costs	
Transition date	

APPENDIX C. - SOFTWARE TRANSFER AGREEMENT

(Customer) agrees to transfer ownership of all rights associated with the software specified in the below table(s). (Customer) acknowledges that it is the rightful owner of this software, and that transfer to DISA Center for Computing Services is permissible under its licensing agreements for the specified software. To the maximum extent possible, (Customer) agrees to provide proof of ownership for all listed software. If applicable, (Customer) agrees to notify software vendors that future license maintenance renewals are to be sent to DISA Center for Computing Services.

DATA ELEMENT	ASSET DESCRIPTION
Vendor	
Product name	
Number of licenses	
Product number	
Version	
Maintenance expiration date	
Pass codes/ keys	

The official signature affixed below reflects understanding and indicates approval by the customer to the requirements and terms and conditions of this Agreement.

For the Customer: (Authorizing Official)

By: ______________________________ Date: _________
Name and Title:

APPENDIX D. - IOC CHECKLIST

DISA IOC CHECKLIST
HW Maintenance
SW Maintenance
ESM Tools
Certification ATO
OS STIGable/Tested
Application tested after STIG
Compliance with Network Security
Port & Protocols & Services for AIS
URL’s defined
Identify any Known Risk

NOTE: The above checklist is the minimum requirements necessary for new workload to achieve IOC. In the event one or more of these items are not completed will affect IOC date