Defense Information Systems Agency
A Combat Support Agency

Defense Information Systems Agency
Enterprise Services Directorate

Terms and Conditions

Applicable to All Service Level Agreements

Published Date:
18 September 2012

Version 4.2

Revision History

Date	Version Number	Section Reference	Changed By	Description
12/2009	3.0	All	CD27	Updates to all sections
4/2012	4.0	All	CD27	Format changes and content updates throughout.
6/2012	4.1	Section 6, Appendix G, Appendix H	ES24	Updated Sect. 6 to reflect the current 10 USC Section 2222 requirements; updated the 10 USC links in App G- References; added App H - Performance Standards.
9/2012	4.2	Section 5, Section 10, Acronyms, Glossary, Appendix I	ES24	Sect 5 - Updated FMLO email Sect 10 – Added note that DEE CMI min charge has changed to $2.5K Added the following acronyms to the acronym and/or glossary lists: ATC, CAP, CCC, CP, ECA, IATO, IECA, IPC, LECA, LIECA, OOB Added Appendix I – GCDS Performance Stds/Responsibilities

Table of Contents

1.0 Introduction

The Terms and Conditions (T&C) constitutes the policies of the Defense Information Systems Agency (DISA) Enterprise Services Directorate (ESD) overarching Agreement with each of ESD's Department of Defense (DoD) Service and Agency partners. The Agreement is made up of the following:

1) Service Level Agreement (SLA) – documents the service(s) ESD is providing to the partner.

   All services provided by ESD shall be documented in an SLA. Services shall be provided in accordance with Department of Defense Instruction (DoDI) 4000.19.

   Stated service levels shall be achieved by the resources allocated to satisfy the partner's projected workload and scheduled priorities. These service levels may be affected if there is a significant workload change or if the partner changes scheduled priorities without advance notice to ESD.

2) Planning Estimate (PE) – estimates the cost for sustainment of services provided to the partner each fiscal year (FY), from the first of October through the 30th of September. The PE is created by ESD for the partner as a planning and budgeting tool for the services ESD provides.

3) Service Catalog – provides descriptions of each service DISA offers, as well as services being developed in the pipeline. ESD shall only provide those services advertised within the Service Catalog that fall under the scope of ESD, and unless otherwise specified in the SLA, these services shall be delivered as described in the Service Catalog.

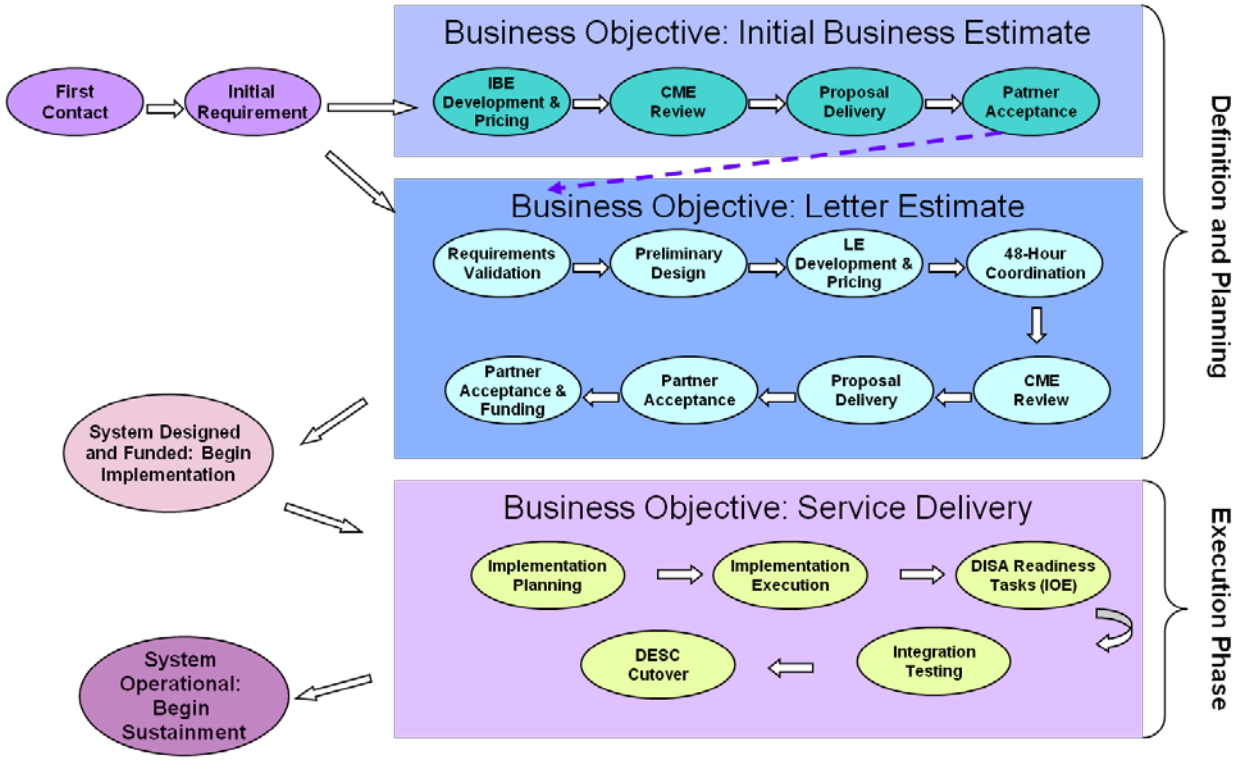
4) T&C – constitutes the policies of ESD's Agreement

Specific services, rates, and costs are outlined in the Agreement. There are links from the SLA to both the Service Catalog and T&C. The content of the Service Catalog and T&C is also considered to be content of the SLA. The information in the Service Catalog and T&C shall not be restated in the SLA.

A Letter Estimate (LE) establishes the basis for, or changes to, the SLA. It is submitted to the partner as a result of a request for new, or changes to existing, workload. The LE restates the partner expectations/mission, requirements, assumptions, and the recommended technical solution. It also includes the estimated cost for implementation and sustainment of the new or changed workload.

The T&C is effective upon partner signature of the LE.

2.0 Business Estimate Process



1) Initial Business Estimates (IBEs) and LEs – While both IBEs and LEs rely on partner 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 partner requirements. An IBE is an option for the partner and may be bypassed altogether in favor of an LE. Target completion timeline for an IBE is 10 working days following the agreement of requirements. The LE is the starting point for new workload, or additions to existing 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 to 45 working days following the agreement of baseline requirements.

2) Process Steps

   a) IBE

      i) First Contact – Initial communication between the partner and ESD. Outcomes include a tracking system entry, tracking number assignment, team/lead assignment, and delivery of service documentation (Service Catalog and T&C) and forms (Service Request Form [SRF]) to the partner.

      ii) Initial Requirement – The ESD Customer Relationship Management Branch (CD2) team lead works with the partner to attain high-level system hosting requirements. Outcomes include a tracking system update, completed (high-level) SRF for IBE development and pricing, and determination (with the Customer Management Executive [CME]) of ability to respond.

iii) IBE Development and Pricing – As described above, the IBE is a method of delivering a quick price estimate to the partner. 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. Outcomes include an IBE, pricing entry, and a tracking system update.

iv) CME or Division Review – All IBEs shall be reviewed at the CME-level or above prior to delivery to the partner. At the division chief's discretion, the 48-hour Coordination (two business days) step may be utilized. Outcomes include an approval or non-approval for delivery along with a tracking system update.

v) Partner Delivery – Formal delivery shall consist of an e-mail or other approved correspondence vehicle that shall allow for a date, time and designated partner to track progress. Outcomes include delivery to the partner and a tracking system update.

vi) Partner Acceptance – The partner wishing to accept or move forward from the IBE should be informed that an LE shall now be developed, which shall involve detailed requirements, a technical solution, implementation planning, and a more explicit price estimate.

b) LE

i) First Contact – Initial communication between the partner and ESD (if the IBE path was not followed). Outcomes include a tracking system entry, tracking number assignment, team/lead assignment, and delivery of the SRF to the partner.

ii) Project Team – The ESD CD2 team lead works with the partner to attain in-depth system hosting requirements and address numerous issues including security posture, network/communication considerations, the partner's integrated milestone schedule, and funding availability. Outcomes include a tracking system update, completed SRF, creation of a solution document for LE development and pricing, Bill of Materials (BOM) initiation, and determination (with CME) of ESD's ability to respond.

iii) Solution Document – ESD team (including appropriate engineering, capacity, operations, communications, and other necessary representatives) develops a general plan for the implementation and management of the partner workload. Outcomes include a solution document, assumptions related to the solution, and a tracking system update.

iv) LE Development and Pricing – The development of the document shall restate partner expectations/mission, detailed requirements, assumptions, and the solution summary. The pricing shall reflect the A-goal and C-goal prices for identified services. Outcomes include an LE and a tracking system update.

v) 48-Hour Coordination – To ensure that a formal proposal from ESD represents an accurate description and pricing of ESD services, coordination with ESD service and financial management teams is mandatory.

vi) CME or Division Review – All LEs shall be reviewed at the CME-level or above prior to delivery to the partner. Outcomes include an approval or non-approval for delivery along with a tracking system update.

vii) Partner Delivery – Formal delivery shall consist of an e-mail or other approved correspondence vehicle that shall allow for a date, time and designated partner to track progress. Outcomes include delivery to the partner and a tracking system update.

viii) Partner Acceptance – The partner wishing to accept the LE should be informed that ESD requires a formal approval, e.g., the signed LE, and initial funding to include the implementation (one-time charges) and initial three months' operating (recurring) funding.

c) Service Delivery – Upon partner acceptance and funding of an LE, ESD shall begin implementation planning and execution to implement the partner's project through Initial Operating Environment (IOE), Initial Operational Capability (IOC), and Full Operational Capability (FOC).

3.0 Management Process Responsibilities

1) ESD and the partner shall furnish all notifications and information to one another in writing via memorandum or electronic mail and by telephone, if urgent.
2) The partner shall work with the appropriate ESD representative to prioritize the partner's applications and to develop the partner's Business Continuity Plan (BCP).
3) ESD shall meet with partner representative(s) as required by the partner, to discuss ESD performance, issues, areas of concern, anticipated workload changes, and any changes or modifications to the Agreement or BCP.
4) To successfully integrate an application into the Continuity of Operations (COOP)/Service Continuity program, there are certain responsibilities which cannot be performed by ESD, including:
   a) Having a DoD Information Assurance Certification and Accreditation Process (DIACAP)-ready application with the partner's Designated Approving Authority (DAA) Authorization to Operate (ATO), etc.
   b) Initiating requests for COOP capability exercises through the assigned Customer Account Representative (CAR). (Exercises are not conducted unless there is a partner request and partner involvement in the verification and validation of the recovery exercise effort.)
   c) Initiating termination or removal of COOP coverage for server-based processing.
5) Exercises of COOP capability require an initiating request from the partner through their assigned CAR.

   Any partner who is not contracting with ESD for COOP/Service Continuity services is specifically excluded from the ESD COOP/Service Continuity program and exercises. No promise or expectation of COOP/Service Continuity is implied or should be inferred. The SLA shall include an annotation that the partner has "No ESD-provided COOP" requirements that are to be satisfied by ESD.
6) ESD CARs shall notify the partner within 180 calendar days of an expiring Certification and Accreditation (C&A) date.
7) The partner shall provide full, detailed documentation for any change requests the partner non-concurs with, providing specifics as to the actual problem(s) the change request would introduce and/or the specific reasons why the change request cannot be implemented at the time it is non-concurred with.
8) When available, ESD Enterprise Services (i.e., Joint Enterprise E-mail [JEE], Joint Enterprise Portal [JEP], Enterprise Content Management) shall be used in lieu of partner-unique application solutions.
9) ESD shall furnish to the partner a primary and alternate ESD point of contact (POC), documented in the SLA, and update these as necessary.
10) The partner shall furnish both the primary and alternate partner POCs to the ESD Service Desk, and update as necessary. In the event the Service Desk cannot contact the primary POC, the

alternate on the list shall be contacted. The partner POC shall notify the partner users of any operational situations that impact service.

11) The partner shall provide estimates of anticipated workloads with which ESD can develop a target budget amount for the PE. ESD shall provide workload history, where it is available, to aid in this estimate.

a) Workload Estimates

i) ESD shall provide the partner with actual mainframe and storage usage information, server, and server storage usage capacity analysis being provided during the year. To develop meaningful projections, the partner and ESD should collaborate, as the partner is ultimately responsible for all mainframe and server projections.

ii) The partner shall notify ESD of in-cycle changes to workload estimates or support requirements as they become known.

iii) The partner shall furnish ESD 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.

iv) ESD shall respond to any in-cycle changes to workload estimates or support requirements after formal notification of such changes by the partner.

b) Budget Estimates

v) The partner uses workload estimate information to submit a budget estimate for funding.

vi) If a difference between the partner budget submission and final approved appropriation exists, ESD, in conjunction with the partner, shall adjust the services in the SLA accordingly, matching services to the partner funding level.

c) SLA Preparation

vii) The SLA shall be specific as to the types and levels of services required.

viii) The partner shall furnish the projected workload for ESD to effect the proper level of support.

ix) The SLA shall contain any additional ESD and/or partner responsibilities that are consistent with the workload rights and support.

4.0 Pricing

The PE is created by ESD for the partner as a planning and budgeting tool for the services ESD provides. The PE serves the following purposes:

1) Sustainment of Existing Workload – ESD shall provide the partner with a proposed PE in the second quarter of the current FY for the following FY. The PE is reviewed by the partner and ESD to confirm that it provides an accurate representation of support provided to the partner. The Partner shall ensure ESD receives a Military Interdepartmental Purchase Request (MIPR) for at least the first quarter of support, as invoiced in the Centralized Invoice System (CIS), by the first of October of the following FY, or immediately upon passage of a Continuing Resolution or DoD Appropriations Act.
2) New Workload or Changes to Existing Workload – Upon signature of an LE, the ESD CAR shall begin creating an SLA for new workload or modifying an existing SLA to reach bi-lateral agreement by FOC. If this modification requires additional funds for sustainment throughout the remainder of the current FY, ESD shall update the existing PE to reflect the change in cost. The Partner must submit funding for implementation costs prior to ESD beginning any implementation of the workload and the Partner is also obligated to provide a MIPR for the amount of the first quarter's increased sustainment.
3) New ESD Partner – Upon signature of an LE, the Partner must submit funding for implementation costs prior to ESD beginning implementation of the workload. 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.

5.0 Funding and Billing

1) Funding – Upon signature of the LE, the partner becomes obligated to pay ESD for the services identified in the LE.

   At the beginning of the FY, funding may be provided contingent on passage of a Continuing Resolution or DoD Appropriations Act, whichever is applicable. The partner shall submit all MIPRs to the ESD Financial Management Liaison Office (FMLO). The FMLO shall submit a MIPR Acceptance Form (DD Form 448-2) to the partner who acknowledges acceptance of the funds received.

   Upon receipt of the MIPR, ESD becomes obligated to provide the services documented in the LE. Within 30 calendar days after the IOE is reached, and no later than FOC achievement, the SLA must be written or modified and provided to the partner. Upon agreement, the partner representative and the applicable ESD representatives shall sign the SLA.

   NOTE: A system reaches IOE when accepted proposals/LEs have information technology (IT) assets that have progressed successfully through ESD implementation and have been turned over to the partner to load their application(s) and data. A system reaches IOC when the application has been loaded, tested, and opened to user base for production. A system is declared FOC when it has been migrated into ESD service and has executed its function for the agreed-to period (30 days after IOC declaration) without critical or high incidents, and it has completed all other defined exit criteria.

   In addition to the dollar amount, the MIPR shall contain the following:

   a) The LE number and funding source

   b) The Treasury Account Symbol (TAS) for both trading partners (ESD and partner)

   c) The partner's Trading Partner Number (TPN)

   d) The Business Event Type Code (BETC) for both trading partners. ESD-issued MIPRs are "DISB" (disbursement) and received MIPRs are "COLL" (collection)

   e) The effective date and duration of the Agreement, to include the expiration of the funding source

   f) The amount and the method of payment

   g) The Business Partner Network (BPN) number for both trading partners

   h) The method and frequency of performance (revenue and expenses) reporting

   i) If applicable, provisions for advance payments and method of liquidating such advances

   j) The parties' rights to modify, cancel, or terminate the Agreement

   k) Accounting/finance office POC information. This includes name, location, telephone number, and e-mail address, as well as: Resource Management Office, Customer Service Office, and Contracting Officer (KO) or KO's Technical Representative (COTR) POC information.

   l) An alternative Dispute Resolution clause

   m) The Billing Account Number (BAN)

n) The SLA number assigned by ESD

o) Where practicable, the application and/or ASC (Block 9)

Funding documents shall be issued and addressed to:
DISA Enterprise Services
Attn: DCH91/FMLO Revenue Team

The mailing address can be found in the partner's SLA and/or LE. When possible, funding documents should be e-mailed to: DISA.Pensacola.ESD.mbx.PEN-MIPRMAIL@mail.mil. MIPR acceptance forms shall be e-mailed to the MIPR originator/issuer.

2) Billing – Routine billing shall commence at the beginning of each FY to reflect services provided. The partner may view invoices online at https://dwfn.csd.disa.mil/CustomerInvoices/default.aspx in the ESD CIS. Current period and year-to-date invoice data shall be updated bi-monthly, reporting actual charges incurred.

The partner shall work with ESD to ensure partner account codes such as CICs, BANs, Industrial Fund Accounting System (IFAS) Codes, Invoice Account Codes (IACs), and ASCs are accurately assigned to capture usage data and service charges at levels useful to the partner.

Partners within the Defense Finance and Accounting System (DFAS) Cleveland Financial Network shall be billed via the Financial Reporting System (FRS) disbursing system. All other partners shall be billed via the Intra-Governmental Payment and Collection System (IPAC). The partner shall promptly review the invoice, and notify ESD of any disputed billings. Subsequent partner billings shall include any adjustments arising from disputed billings.

If the bill payer changes, the funding responsibility for an existing workload remains with the originating bill payer until the FMLO receives written notification of the new bill payer, the effective date, and a MIPR from the new bill payer. ESD and the FMLO should receive this data at least 30 business days prior to the effective date. ESD shall change the appropriate CIC upon receipt of the new information, and shall document this information in the partner's SLA.

a) Server and Storage

i) The recurring rate-based billing of a new server or operating environment (OE) and the raw storage, for new partner workload, begins at the time a server or OE is handed over to the partner for logon. This typically occurs at IOE. IOE is defined as the point when ESD has completed the initial system implementation (e.g., hardware installation, storage allocation, operating system [OS] load, Security Technical Implementation Guide [STIG], etc.). At IOE the system is turned over to the partner to load their application and test the system. One-time implementation costs are also billed to the partner at this point.

ii) For OEs that have undergone a technical refresh, when the new hardware is declared IOE, ESD allows 30 days for parallel processing before the old environment is turned off. It allows for both sets of hardware to run parallel, with only one set billing, while any technical issues regarding the transition are resolved. At the end of the 30-day period, if the partner is not ready to decommission the refreshed hardware; both sets of hardware and raw storage shall be billed.

6.0 Business Management Modernization Program

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). The partner must provide the Business Management Modernization Program (BMMP) documentation required by United States Code (USC), Title 10, Section 2222 to the Office of the Secretary of Defense (OSD) Defense Business System Management Committee (DBSMC) (established by USC, Title 10, Section 186). The partner is responsible to submit a copy of the DBSMC certification results or certification control number for the proposed business system to ESD prior to ESD obligating funding for services. Failure to present the appropriate documentation precludes ESD from taking further action or providing services until the time documentation is submitted.

Funds available to the DoD, whether appropriated or non-appropriated, may not be obligated for a defense business system program that will have a total cost in excess of $1,000,000 over the period of the current future-years defense program submitted to Congress unless—

1) The appropriate pre-certification authority for the covered defense business system program has determined that—

   a) the defense business system program is in compliance with the enterprise architecture developed under subsection I and appropriate business process re-engineering efforts have been undertaken to ensure that—

      i) the business process supported by the defense business system program is or will be as streamlined and efficient as practicable; and

      ii) the need to tailor commercial-off-the-shelf systems to meet unique requirements or incorporate unique interfaces has been eliminated or reduced to the maximum extent practicable;

   b) the defense business system program is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or

   c) the defense business system program is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect;

2) the covered defense business system program has been reviewed and certified by the investment review board established under subsection (g); and

the certification of the investment review board under paragraph (2) has been approved by the Defense Business Systems Management Committee established by section 186 of this title. Documentation for above must be provided as part of the partner's acceptance of any BMMP solution offered by ESD before implementation of the project can proceed.

Business Transformation Agency (BTA) Investment Review Boards (IRBs):
http://www.bta.mil/products/irb.html

IRB frequently asked questions (FAQs):
http://www.bta.mil/products/Investment%20Review%20Process%20FAQs.pdf

7.0 Duration and Termination of Agreement

1) Duration – The SLA between ESD and the partner shall have an indefinite lifespan. It shall be reviewed annually at a minimum, ensuring ESD is furnishing all the negotiated IT services required by the partner. The annual review provides a forum for the partner to identify future workload requirements or other required changes which shall be recorded in the SLA and corresponding PE.

   The review timeframe recommendation is to perform annual reviews concurrently with PE issuance to partners and/or within 30 calendar days of a support change implementation. New workload, or changes to existing workload, requires a new SLA or modification to an existing SLA upon achievement of FOC.

2) Termination – Termination shall be conducted in accordance with guidance provided in DoDI 4000.19 requiring 180 calendar days written notification. ESD shall discontinue service as soon as reasonably achievable, but billing may continue for up to six months for actual costs or services provided during the six months. Termination charges may be applied to the partner per the Financial Management Regulation, Volume 11B, chapter 11, paragraph 110102.

   With assistance of the ESD CAR, the partner shall provide a completed Agreement Termination Worksheet (Appendix A).

8.0 System Technology

1) System Architecture – The information assurance (IA) architecture is defined to meet, at a minimum, the service requirement for the Mission Assurance Category (MAC) II, Sensitive, Medium Robustness, system configuration, network configuration and partner support requirement identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 and DoDI 8500.2.

   a) Server – The standard Server Enterprise Architecture (SEA) is a set of minimum requirements for a server to be placed in an ESD environment. These standards were developed by taking into account best practices, network requirements, storage requirements and overall general knowledge of the Defense Enterprise Computing Center (DECC) environment.

   b) Storage – The Storage Enterprise Architecture (SEA) is based upon the DoD Joint Technical Architectural (JTA) Framework Version 6.0. The DoD JTA Framework was developed in accordance with the Global Accounting Office (GAO) Enterprise Architecture Management Maturity Framework and is maintained in the DoD Information Technology Standards Registry (DISR).

2) Configuration

   a) Server – There are four main core hardware server platforms in ESD:

      i) Reduced Instruction Set Computing (RISC)-based servers from Sun, Hewlett-Packard (HP), Fujitsu and IBM

      ii) Itanium based servers from HP

      iii) Mainframes from IBM and Unisys

      iv) x86-based servers from multiple vendors such as DELL, IBM and HP

      The capacity services contracts provide hardware and OSs that include HP Windows, HP UNIX, Sun Solaris, Unisys, and IBM OS systems.

      ESD uses virtualization technology for server workload. In the Intel™ space this is 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); Dynamic Resource Scheduling (DRS), which is the capability to place up to 32 physical servers into 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 and vendor partitioning methods are varied, but the following is a basic description: Physical or hard partitioning subdivides a single server, such that all power, Central Processing Units (CPUs), memory, and Input/Output (I/O) devices used by a partition are dedicated to that partition and no other. A physical partition has the following characteristics:

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

vi) CPUs and memory are allocated to the partition based on hardware configuration and cannot be shared with another partition or be dynamically reallocated.

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

viii) May be configured as a single OS, or host multiple virtual OSs.

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 (CPU, memory, and I/O) can be shared between the virtual partitions, either dynamically by the operator, or during boot-up configuration.

b) Storage – disk and tape technologies are the major data storage technologies used to support all OSs.

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

x) Traditional and virtual tape is used for backups, archives, and for those files that do not need to be immediately accessed.

The foundation of the architecture is a high-speed Core/Edge Storage Area Network (SAN) consisting of fibre channel (FC) switches and directors connecting servers to their storage devices at each processing location. However, in special cases, with associated documentation, ESD can deploy Network Attached Storage (NAS) solutions. The SAN provides all standard storage functionality such as mirroring, data replication, data snapshots, data archiving, data de-duplication, 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 are low cost and highly reliable. Each device can support all OS environments on the SAN. Assured computing techniques are designed into every SAN. SANs exist at all processing locations although some are managed remotely from a Systems Management Center (SMC).

ESD Enterprise Backup Network (EBN) employs a high speed Internet Protocol (IP) based network with automatic tape libraries to support the data backup and archiving process. ESD has an off-site tape storage contract for safe and efficient tape storage. Symantec (Veritas) NetBackup is the software used for backup.

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 OS level.

9.0 Ownership and Licenses

1) Data – As the service provider, ESD is required to certify and accredit the platforms/systems operating in the DECCs. The partner operating applications on the systems within the DECCs is required to certify and accredit the applications as the owner of the data processed/produced in these applications.

2) Hardware

   Effective the first of October, 2011, ESD no longer accepts partner-owned hardware. Partner-owned hardware already residing in ESD DECCs shall be grandfathered until those hardware assets have reached end-of-life, at which time ESD shall provide a technical refresh of those assets from ESD's Capacity Services contracts.

   ESD has negotiated a series of indefinite-delivery/indefinite-quantity capacity services contracts to obtain Unisys and IBM mainframes and Windows/Linux, Solaris and UNIX servers.

   ESD is responsible for all equipment within the DECC. ESD manages, tracks, and maintains accountability for this equipment. These ESD responsibilities are covered by the basic services provided to the partner, and include establishing and maintaining auditable accountable records in the Defense Property Accountability System (DPAS), capitalizing and depreciating assets requiring capitalization, maintaining supporting documentation, hand receipting, and performing annual physical inventories and reconciliations.

   a) Maintenance Support – ESD requires a standard level of maintenance support for all assets owned and maintained by ESD. Maintenance support is based on DoDI 8500.2 MAC requirements. MAC I/II systems require 7/24/365 support, with a two (2) to four (4)-hour response time for maintenance and immediate response on parts. Maintenance support for MAC III systems is defined as next business day with same day parts arrival.

   b) Partner/Vendor-Owned Hardware Assets

      ESD does not provide property accountability services for partner or vendor-owned assets. It is incumbent upon the owner of the assets to meet all DoD regulatory or partner-specific property accountability guidance that may apply. ESD shall track in CORAS partner/vendor-owned assets for contractual purposes only and shall annually inventory partner/vendor-owned property. Partner/vendor property custodians, upon request, may request current partner/vendor-owned inventory reports.

3) Software – ESD must acquire, own and maintain all executive software. Application software, unless otherwise discussed below or for solutions under our "As a Service" model, is owned by the partner. The partner is responsible to abide by all license terms and conditions imposed by End User License Agreement (EULA). The partner is responsible for the license management and any/all compliance issues that might arise. If the partner is proposing to provide their own executive software, the executive software licenses must be transferred to ESD. No executive software is permitted to operate on an ESD mainframe or server that is not ESD-owned.

   a) Executive Software

      xi) Scope – for purposes of ESD software management, the scope of executive software has been defined as: The basic OS, utilities, tools and other commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software products used to control and manage the

execution of applications and their interaction with the hardware configuration. Executive software allows the processing of specified data against an application to produce the intended results.

xii) Management – ESD shall perform installation, maintenance, and technical support for executive software packages. ESD shall maintain the most current version, licensing documentation, and release levels acquired under existing contract maintenance terms. ESD shall apply service packs, hotfixes, security releases and other patches as appropriate. Activities related to the sustainment of executive software shall be coordinated with the partner.

b) Application Software

xiii) Mainframe (IBM or Unisys) – On behalf of the partner, ESD shall procure the necessary executive software to allow the application software to run, and shall charge the partner directly for the cost.

xiv) Server – Any application software that is not bundled in the server rate shall be directly charged to the partner.

c) Software Transfers

xv) Mainframe – Mainframe software is not generally transferable unless approved by the software vendor.

xvi) Server – Server software is generally transferable with vendor approval. It is the responsibility of the current owner to provide proof of ownership and to ensure that licenses are transferable. Any fees associated with a contract/Agency transfer shall be charged to the partner accordingly. The licenses must be under a current maintenance agreement and the use must be in accordance to the vendor's current EULA.

xvii) If the partner is proposing to provide their own software for transfer to ESD, the following guidelines are required to ensure that appropriate, uninterrupted maintenance support is provided for the software. The following items are required in order to effect the transfer:

(1) A completed, signed Software Transfer Agreement (Appendix B) submitted to ESD.

(2) A completed table of data elements for each software license/maintenance agreement being transferred.

(3) 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.

(4) Any media containing original or backup copies of the software, which could be of use to ESD.

(5) For software currently covered under a renewable maintenance contract, please notify your ESD CAR to change the address for renewal notification.

10.0 Security and Access

1) Automated Information Systems (AISs)
   a) AISs hosted within ESD environments must maintain compliance with DoD and Joint Staff regulations, US CYBER Command directives and guidelines, and other proper authority. (See Appendix F – References.)
   b) AISs must have a current accreditation (ATO), Interim ATO (IATO), or Interim Authority to Test (IATT) to enter ESD production environments. Systems operating with IATT shall not be used for operational purposes. (ref. DoD 8510.01, sec. 6.3.3.2.6.3.3.)
   c) All AISs shall be hosted and monitored using ESD-provided capacity and ESD-supported OSs.
2) Web and application servers must be operated in separate environments from databases. Web and application servers should be separated, when possible.
3) All network traffic in and out of ESD facilities shall traverse the Demilitarized Zone (DMZ).
4) Data sharing or manipulation across partner applications is prohibited, unless agreed upon by all parties and documented in the SLA(s).
5) Destruction of storage media shall be conducted in accordance with ESD local policy and procedures.
6) Root Access Limitations
   a) Partner Root access is only allowed when an AIS is in an approved Test and Development (T&D) environment. Partner Root access shall be revoked before an AIS is promoted into a DECC production environment. The partner may be granted certain limited privileged access as determined by the ESD Chief Information Officer (CIO).
   b) The partner requiring full Root access to a production AIS must have the application moved into a T&D environment before access is enabled.
7) Application Monitoring – Application audit logs and network traffic must be monitored in accordance with STIGs. The OS administrator must have access to application logs.
8) Computer Network Defense (CND) – All AISs must maintain CND service capabilities to continuously protect, monitor, detect, analyze, and respond to unauthorized activity during all operating hours of the system.
9) Classified Information Incidents (CIIs) – CIIs occur when classified information is introduced to a system above the level of classification for which the system is accredited. Partner organizations that cause CIIs within ESD hosted environments shall be held financially liable and shall be billed for all accumulated restoration costs incurred by ESD, but not less than $5,000 per incident.

   NOTE: The minimum amount charged to ESD partners for DoD Enterprise Email (DEE) Classified Message Incidents (CMIs) has been changed from $5,000 to $2,500.
10) Roles and Responsibilities are as defined below, unless otherwise documented in the SLA.
   a) Enterprise Services – The roles and responsibilities below do not apply to applications wholly owned and operated by DISA or ESD and offered as a service to the partner. (e.g. JEE) For these services, DISA or ESD retains responsibility for IA and compliance. The partner is responsible for reporting any security incidents that affect these systems. (e.g. spillage)

b) Shared Responsibilities

i) Overall security is shared between the DISA DAA and the DoD Component DAA.

ii) IA and Compliance Validation of AISs hosted within ESD environments is shared between ESD and the partner.

iii) CND is shared between ESD and the partner.

iv) ESD has identified the Inherited IA Controls in Appendix D and created the Enterprise Negotiated IA Controls that apply to each partner. Any exceptions must be vetted and approved by the DISA Mission and Assurance Branch within the ESD CIO Office, and documented in the SLA. Links to the Negotiated IA Controls identified by MAC level shall be provided to the partner acquiring ESD services.

c) ESD Responsibilities

i) Security of all ESD-owned and controlled technical environments that supply services (i.e., during transport, processing, and storage on ESD platforms and servicing networks). ESD certifies to the partner that the required security mechanisms are present and operational in accordance with DoD and Joint Staff regulations and US CYBER Command directives and guidelines.

ii) Maintaining security compliance for all ESD hosted OSs.

iii) Fully implementing all DoD IA Controls including those DoD IA Controls documented within the applicable technology platform-specific DoD STIG in accordance with DoD IA policy.

iv) Maintaining a Personnel and Information Security Program to ensure access is in accordance with applicable DoD security directives.

v) Maintaining a system for managing access control to the OS and its supporting utility software.

vi) Applying all Vulnerability Management System (VMS)-related security fixes and vendor-recommended software maintenance to all OEs and applications managed by ESD.

vii) Incident Reporting

(1) Notifying the partner of any suspected or known security deviations or violations.

(2) Immediately directing any security incidents through ESD security channels and notifying the partner (if affected by the incident).

viii) C&A

(1) Maintaining C&As for all DECCs.

(2) Upon request, providing a copy of the hosting DECC's DAA-signed accreditation memo and DIACAP Scorecard to the partner to validate satisfaction of controls for which ESD has responsibility.

(3) Providing IA consulting services for C&A and VMS issues.

(4) Documenting COOP responsibilities assigned to ESD, developing recovery processes to be executed by ESD, and participating with the partner who pays ESD for COOP services in COOP exercises of those processes.

ix) Application Monitoring – If ESD manages an application, ESD shall provide monitoring of application audit logs and network traffic in accordance with STIGs.

x) CND – ESD provides certain Tier 3 CND capabilities 24 hours a day as described in Appendix C – Computer Network Defense.

xi) Other Compliance Issues – ESD shall implement an acceptable Risk Management Plan, and any other applicable Federal, Departmental and/or Agency policies, guidelines or requirements that are provided in writing by the partner. (i.e. Common Criteria, Health Insurance Portability and Accountability Act [HIPAA], Privacy Act).

d) Partner Responsibilities

i) VMS and Enterprise Mission Assurance Support Service (eMASS) data entries for the partner's AIS.

ii) The partner's Program Manager (PM) is responsible for following Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01. The PM shall monitor and respond to IA Vulnerability Alerts (IAVAs) and provide ESD with a software release or mitigation plan. The PM should monitor the application security patches from the vendor and provide releases to ESD. Security patches from the vendor should be no more than one (1) generation old.

iii) The partner's PM shall review and respond to any IA related change requests initiated by ESD. In the event the partner non-concurs with an IA change request, the partner shall provide, via their DAA, full specific documentation on why they are non-concurring with the change request. Such documentation shall provide the complete and specific actual problem(s) that would be introduced by implementing the IA change, any potential suggested alternatives, alternative dates for implementing the IA change, etc. This is required at the time the change request is non-concurred. Failure to provide specific and detailed documentation for the non-concurrence of an IA change request shall result in the approval and implementation of the change request.

iv) Security tasks related to AIS components that ESD is not contracted to support. (This includes, but is not limited to, database administration, web administration, and application support.)

v) Ensuring control of all data retrieved from within ESD technical environments and for the security of any and all partner-owned and controlled technical environments. Partners shall provide certifications to ESD that their security mechanisms are present and operational.

vi) Incident Reporting

(1) Partners shall notify ESD of any suspected or known security deviations or violations involving systems hosted with ESD.

(2) Partners shall immediately direct any security incidents through partner security channels and ESD (if affected by the incident).

vii) Obtaining and maintaining AIS C&As.

viii) Application Monitoring – Partners shall monitor application audit logs and network traffic in accordance with STIGs, unless ESD application management services are provided.

ix) CND

(1) Partners are responsible for ensuring comprehensive CND services exist and are operational.

(2) Partners are responsible for all CND services not explicitly provided by ESD.

x) Other Compliance Issues – Partners shall 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.

xi) Developing applications that interface and exchange identification and authentication with the security products utilized by ESD and the DoD-sanctioned STIGs and Application IA Controls in accordance with DoDI 8500.2.

xii) Partners with 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 ESD.

xiii) Coordinating with ESD on any Exceptions to Normal Processing as soon as they become known. ESD shall respond to partner requests for Exceptions to Normal Processing within 10 calendar days after formal notification. Exceptions to Normal Processing are defined in the Glossary. Normal Processing services are specified in the SLA.

xiv) Furnishing both the primary and alternate partner POCs to the ESD Service Desk, and updating as necessary. In the event the Service Desk cannot contact the primary POC, the alternate on the list shall be contacted. The partner POC shall notify the partner users of any operational situations that impact service.

xv) Coordinating with ESD representatives to prioritize the partner's applications and to develop the COOP plan.

xvi) Maintaining access control for users to their applications.

xvii) Furnishing all notifications and information to ESD via memorandum or electronic mail; and by telephone, if urgent, to confirm receipt.

xviii) Making appropriate modifications to applications in support of periodic executive software and hardware upgrades.

xix) Partner applications referring to hard-coded IP addresses must be changed to Domain Name Server (DNS) addresses where possible.

xx) Allowing ESD sufficient administrative rights and privileges to apply all VMS-related security fixes and vendor-recommended software maintenance to partner-owned equipment residing in ESD DECCs.

NOTE: ESD policy states that ESD shall no longer accept partner-owned equipment after the first of October, 2011. Partner-owned equipment currently residing in ESD DECCs

shall be grandfathered until end-of-life and technical refresh. (Ref. Section 9.0 Ownership and Licenses.)

xxi) Providing the following IA information for the partner's AIS and notifying ESD in writing of any changes to this information.

(1) Certifiers Recommendation Statement and Accreditation Letter

(2) Residual Risk identified in an Acceptance of Risk Statement or Memo

(3) An Application Security Review Checklist and Application STIGs for:

(a) Database (if partner-owned)

(b) Web (if partner-owned)

(c) Application (if partner-owned)

(4) Compliance Assessment IA Vulnerability Management (IAVM) and Reporting must be completed. Security Test and Evaluation (ST&E) must be completed if required.

(5) Plan of Action and Milestones (POA&M) identifying any Open Vulnerabilities (Residual Risk)

(6) Results from Application STIG and Application Checklist

(7) Ports, Protocols, and Service Management (PPSM) Registration

(a) The partner shall register all ports, protocols, and services for the partner's AISs via https://pnp.cert.smil.mil.

(b) The partner shall provide ESD with the partner's confirmation e-mail from PPSM

(c) Unidentified ports shall be accompanied with pertinent mitigations

(8) Network Topology (provided by hosting DECC site or in accordance with the Unclassified/Classified Connection Approval Office [UCAO/CCAO] template)

(9) Registration in appropriate databases (DoD IT Portfolio Repository [DITPR], VMS, eMASS, Secure IP Router Network [SIPRNet], GIG IA Portfolio [GIAP] System)

11.0 Additional Responsibilities

1) ESD shall determine hosting and management sites.
2) The partner shall submit any specialized or additional communications support requirements 120 calendar days in advance for Automated System Interruption (ASI) and 7–10 business days for general requirements. Urgent requirements shall be handled on a case-by-case basis. All ASI requests must be submitted to the supporting Service Desk.
3) The partner shall test all new releases prior to releasing into the production environment. The partner shall release testing to ESD if requested.
4) ESD shall notify the partner of:
    a) Changes to established hours of processing or service availability
    b) Scheduled downtimes or other restrictions to processing or service availability, at least 72 hours in advance
    c) Hardware and software upgrades, releases, and changes which may impact the partner
    d) Any suspected or known security deviations or violations

12.0 Dispute Resolution

An alternative Dispute Resolution clause is as follows:

1) Dispute resolution shall involve the program offices, resource management office, accounting offices, KO, and agency's Chief Financial Officer (CFO), as appropriate. Disputes shall be documented in writing with clear reasons for the dispute. A Memorandum of Agreement (MOA) shall be signed by the CFOs of each department and agency to acknowledge the active participation of that department or agency 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 the following paragraphs. Disputes are of two types: accounting treatment (e.g., of advances, non-expenditure 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 a charge is disputed to agree on the treatment of an accounting entry. If agreement cannot be reached, both trading partners' CFOs shall request that the CFOs Council's Intragovernmental Dispute Resolution render a final decision.
    b) If Intragovernmental differences result from contractual disputes, the trading partners have 60 calendar days from the date a charge is disputed 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 shall 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 is cause for a contractual dispute. The partner 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 partner's threshold, and the partner elects not to pursue a dispute, then the partner shall pay the amount.

When it appears that an SLA has been breached by either party, ESD shall identify the circumstances behind the incident. The resolution could take many forms (i.e. a Service Improvement Plan [SIP] that is referred to the ESD Problem Management team or a modification to an SLA).

Appendix A – Termination Worksheet

To access this form for use, please click HERE. If you do not have a Partner Portal account, please request this form from your CAR.

This worksheet is needed only if one of the following occurs:

1) Eliminating ESD support/entire SLA
2) Decommissioning entire application/ASC

This worksheet is not needed, but ESD must still be notified, if:

1) The partner is declining an existing option
2) The partner wants to de-install existing hardware

DISA Enterprise Services Termination Worksheet	
Partner Name:	
E-mail:	
1. Application System Code (ASC):	
2. Data System Designator (DSD) if applicable:	
2.a. 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).	
Date(s):	Site(s):
Date(s):	Site(s):
Date(s):	Site(s):
Date(s):	Site(s):
Date(s):	Site(s):
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):

DISA Enterprise Services Termination Worksheet	
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. CME Team Project Lead/Manager: (name and phone number)	
11. Date CME Team Project Lead/Manager 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:	

DISA Enterprise Services Termination Worksheet		
19. Identify any software unique to this ASC/DSD that is no longer needed:		
20. Identify other billable items for which service is no longer required such as Certification Authority (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:	Date:	
24. Partner Management Division		
Name:	Office Symbol:	
Phone:	Fax:	
E-mail:		
Signature:	Date:	
25. Resource Management Division		
Name:	Office Symbol:	
Phone:	Fax:	
E-mail:		
Signature:	Date:	

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

Appendix B – Software Transfer Agreement

To access this form for use, please click HERE. If you do not have a Partner Portal account, please request this form from your CAR.

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

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 partner to the requirements and terms and conditions of this Agreement.

For the partner: (Authorizing Official)

Signature: _____

Date: _____

Printed Name: _____

Title: _____

Appendix C – Computer Network Defense

ESD employs a documented reporting structure designed to alert managers and administrators at all levels concerning IA. Timely collation, correlation, information analysis, and warning dissemination require a robust reporting structure. Automated analytical tools and alerts of attacks in progress are essential to the IA process. This reporting structure shall also be linked to intelligence, law enforcement, policy makers, and the Regional or Theater-level information systems (IS) community (both government and commercial). Coalition Network Operations (NetOps) Centers (CNCs)/Theater NetOps Centers (TNCs) incident reporting procedures shall consider the information needs of the intelligence and operations communities for planning, coordinating, and implementing response options.

The following are the main CND functions:

1) IA, Incident Status, and Operations Mission Impact
   a) Incident/event detection and response
   b) Site/regional-level sensor data review
   c) Level I data analysis – Data entry and initial log review
   d) Level II area of responsibility (AOR) data – Correlation of activity with sensor data
   e) Incident/event –Network outage correlation
   f) AOR incident/event trending
   g) Anti-virus software support – Assist with download, setup, and configuration
   h) Coordination between CNCs/TNCs, other certifications (CERTs), Continental United States (CONUS) Theater Network Operations and Security Centers (CTNOSCs), DISA IA representatives, Service Theater CERTs, and Cyber Command

2) Provide Reports and Feedback on Events and Incidents to the Lowest AOR Level
   a) Customer Support Desk for IA
   b) Hotline operations for IA
   c) Incident, event, mission impact determination, escalation, and prioritization
   d) Countermeasures
   e) Incident/event coordination
   f) Feedback to the partner

3) 24x7 Combatant Command (COCOM)/DOD Agency Intrusion Monitoring
   a) Sensor monitoring
      i) Continuous operations
      ii) Retrospective and real-time
   b) Assist COCOMs in battle damage repair
   c) Response/recovery courses of action (COAs)
   d) Preventive countermeasures
   e) System administrator (SA) actions
   f) Signature updates to the sensors

4) Maintain a Partner Profile
   a) Sensor configuration
   b) 24-hour POC
   c) 24-hour leadership information and notification

d) IA manager (IAM)/IA Officer (IAO)
e) Network diagrams

5) Produce AOR Daily/Weekly/Quarterly Reports
   a) Daily
      i) Report daily events/incidents
      ii) Update status of past events/incidents
      iii) Operational status of sensors
   b) Weekly
      i) Show AOR trends
      ii) Correlation of events/incidents/malicious code
   c) Quarterly – Show AOR trends
   d) As Needed
      i) Distribute information on new IAVM
      ii) Distribute information on new threats/malicious code/tools/techniques

6) Support and Participate in COCOM IA Exercises
   a) Coordinate with COCOM exercise planners
   b) Request support from CYBER COMMAND and Field Security Operations (FSO)
   c) Coordinate all exercise support with CYBER COMMAND and FSO
   d) Coordinate all vulnerability assessments with CYBER COMMAND and FSO

The following are the CND roles and responsibilities:

1) Protect
   a) Vulnerability Analysis and Assessment (VAA) Support
      i) ESD shall:
         (1) Assist the partner with identifying the need for Vulnerability Assessments (Vas), the most appropriate type of VA, and possible sources for Vas. Utilizing a formal process, assist the partner with internal/external VA by providing technical assistance, reporting requirements and situational awareness.
         (2) Conduct bi-annual external VAA scans and provide results to partner (DISA shall obtain written permission from the partner's DAA before executing VA tools, and shall maintain copies of these documents in their files). Using documented policies and procedures, test and evaluate VA tools on their effectiveness, appropriateness and safety prior to use on partner systems in order to provide for the safeguarding of these systems.
         (3) Ensure vulnerability data obtained from VAA activities is analyzed to determine potential impacts to partner network operations, and assist partner in identifying and mitigating findings identified.
         (4) Monitor partner's corrective actions or mitigation strategies. Receive and maintain written confirmation of implementation from partner.
         (5) Maintain current IP database
      ii) Partner shall:
         (1) Develop and implement a VAA compliance program that supports the Joint Task Force – Global Network Operations (JTF-GNO) Chief Technology Officer (CTO)

08-005, Directive for Automated Scanning, Remediation and Reporting of Network Vulnerabilities.

(2) Utilize the DoD VMS for vulnerability scan data storage, granting access to specific DISA personnel for vulnerability analysis and correlation.

(3) Maintain current knowledge of policies and procedures for conducting vulnerability scans, notification processes, tools implementation, and how to operate and abort scan tools if necessary.

(4) Assist DISA with obtaining written permission from the DAA to conduct external VA scans, and retain a copy of these documents.

(5) Acknowledge, maintain and reference DISA's vulnerability mitigation recommendations and/or provisioning of technical assistance, and any implementation of recommendations.

(6) Provide copies of any vulnerability assessment trend analysis to DISA if and when available. Analysis may include: increase/decrease in number of vulnerabilities observed, changes in types of vulnerabilities, and/or recurring vulnerabilities.

b) Red Team Support

i) The partner may subscribe for DISA FSO CND services or the partner shall provide a focused Red Team assessment and notify DISA DAA and ESD trusted agents prior to Red Team activities.

ii) The partner shall:

(1) Develop a formal program to periodically request and allow the conduct of external Red Team assessments. Maintain locally, and share the results of all such assessments with DISA.

(2) Develop formal procedures for incorporating lessons learned from Red Team assessments into mitigation strategies, policies, and risk assessments.

c) Malware Protection Support

i) ESD shall:

(1) Provide Anti-virus/Anti-Malware software and updated signatures for NIPRNet and SIPRNet. Through subscription to the ESD-Network Assurance (ESD-NA) virus list server, and other anti-virus organizations, provide warnings and updated information on malicious (spyware, viruses, Malware, adware, etc) code threats.

(2) Maintain a 24 hours a day, seven days a week (24x7) virus response capability, and respond in a timely manner to all partner reports of virus activity or requests for support.

(3) Maintain a current POC list for DoD-approved vendor support.

(4) Monitor Host Based Security System (HBSS) asset awareness and compliance data to ensure partner assets are running updated anti-virus engines and signatures.

(5) Conduct weekly anti-virus scans of network-connected devices in accordance with the DoD STIGs and develop/implement a program to identify infected assets and coordinate with the partner to rebuild, quarantine, or remove the asset from the network upon detection.

ii) Partner shall:

(1) All ESD to implement anti-virus/anti-Malware software and maintain updated signatures for all NIPRNet and SIPRNet systems.

(2) Ensure that all CND personnel are aware of DISA's 24x7 capability to assist with Malware mitigation, and maintain an up-to-date listing (NIPRNet/SIPRNet e-mail, phone, Secure Telephone Equipment (STE), etc.) for contacting the applicable DISA CNDSP Tier 2 Provider.
(3) Ensure that personnel understand how to conduct timely reporting of the detection of unknown/emerging Malware to DISA.

d) INFOCON Implementation
i) ESD shall:
(1) Maintain the latest DoD guidance and procedures for the INFOCON reporting process, formats, directive actions, and security.
(2) Provide notification to the partner of all changes to the global and Theater (where appropriate) INFOCON level, and recommended actions in response to any changes to the INFOCON level or Targeted Response Options (TROs). Monitor subscriber INFOCON status, and advise DCC of any changes.
(3) Provide guidance and recommend tabletop exercises at least annually to the partner on directed measures to protect their networks in response to INFOCON levels five (5) through one (1).
ii) The partner shall:
(1) Ensure that all partner organizational elements implement appropriate INFOCON levels. Immediately notify DISA of any partner-directed change in INFOCON level or TROs.
(2) Maintain the latest DoD guidance and procedures for the INFOCON reporting process, formats, directive actions and security.
(3) Provide a read-only view in VMS of assets and POC information to DISA for situational awareness of vulnerability status and mitigation strategies.

2) Detect

a) Network Security Monitoring/Intrusion Detection ESD-NA (Tier 2)
i) ESD shall:
(1) Utilize formal network security monitoring policies and procedures that include the appropriate use of DoD-approved Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) tools that have automated alert capabilities enabled.
(2) Perform Detection (Monitoring and Analysis) activities on the CCSDs using intrusion detection/prevention systems (IDS/IPS), hereafter called sensors. Activity shall occur on a 24x7 basis.
(3) Utilize partner sensors if determined feasible. Partner-provided sensors should be of the same technology currently in use by DISA at other locations.
(4) Follow documented procedures for characterizing anomalous events detected by sensors and other network monitoring systems.
(5) Monitor the partner's unclassified and classified networks. Provide failover COOP of monitoring activities in the event of an outage at the service provider location when COOP is being provided.
(6) Review and analyze logs in a timely manner to detect intruders, and within 30 minutes of detection of an event to begin preliminary analysis of the event.

Follow documented procedures to obtain copies of the partner's audit/system logs.

(7) Monitor and analyze HBSS critical alerts, utilizing correlation capabilities with other Tier 2 network-based monitoring event data.

b) Attack Sensing and Warning (AS&W)

i) ESD shall:

(1) Give the partner notice of suspicious/malicious network traffic or similar activities that suggest an impending or on-going attack. General warnings of potential computer attacks shall also be provided to the partner. Limited impact assessments and recommendations to configurations and/or rule sets may be provided based on threat data.

(2) Search for and analyze low-level ("low and slow") events to identify possible unauthorized activity utilizing exploratory problem-solving or self-learning techniques. Suspicious/significant activity shall be shared among the CND/IA community.

(3) Distribute documented guidance on an annual basis of best practices that support an overall DoD policy for configurations or rule sets.

(4) Follow documented procedures to collaborate with other CNDSPs to compare and exchange notes, analysis reports and other information on intrusions, attacks or suspicious activities.

ii) The partner shall:

(1) Ensure that AS&W information is appropriately disseminated to the partner and the partner's sub-components.

(2) Acknowledge, maintain and reference all DISA warnings and indications messages and security configuration guidance.

(3) Coordinate awareness of current activities occurring in the partner's environment (Red Team, law enforcement, counterintelligence, exercise, etc.) and relay in a timely manner the potential impact they may have on DISA's ability to conduct effective network defense monitoring.

(4) Share any internal or command analysis, information or warnings pertaining to intrusions, attacks or suspicious activities to DISA for situational awareness.

c) Indications and Warning (I&W)/Situational Awareness

i) ESD shall:

(1) Develop tactics, techniques and procedures to provide the partner with intelligence-based potential computing threats and expected imminent actions on a timely basis. These warnings shall be based on the Intelligence Community and other sources. Situational awareness shall also be provided to the partner based on Theater activities and those threats and activities correlated from other entities (i.e., DCC, Global NetOps Support Center [GNSC], and TNCs).

(2) Follow a documented methodology for sharing information with the Intelligence Community via proper channels, and for checking non-governmental and counterpart CNDSP organizational websites for threat and warning notifications daily to ensure situational awareness.

(3) Coordinate within DISA and with the partner to consolidate and correlate Situational Awareness data into a single integrated picture (in accordance with the

Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement [CCER] NetOps Concept of Operations [CONOPS]).

ii) The partner shall:
(1) Acknowledge, maintain and reference any threat reports disseminated by DISA or other sources.
(2) Ensure I&W and Situational Awareness information is appropriately disseminated within the organization, and that daily command situational awareness is shared with DISA.

3) Respond

a) Incident Reporting
i) ESD shall:
(1) Report detected events and potential incidents that occur on ESD-NA monitored sensors using documented procedures in accordance with DoD guidance. These events/incidents shall be provided to the partner and reported to DCC.
(2) Ensure incidents are populated into the Joint CERT Database (JCD). ESD-NA is the conduit to DCC for all CND incidents.
(3) Follow documented policies and procedures for handling incidents reported to law enforcement and counterintelligence agencies.
(4) Retain all incident reports (electronic or paper) for at least one year.
ii) The partner shall:
(1) Develop and implement a process with formal documented procedures to conduct incident handling in accordance with DoD/CJCS incident handling procedures.
(2) Self-report all incidents and questionable events for covered networks in a timely manner to DISA as discovered. DISA shall enter incidents into JCD on behalf of the partner.
(3) Verify or validate incidents identified by DISA, along with any operational impact, and provide feedback to DISA in a timely manner.
(4) Retain soft or hard copies of all applicable incident reports for one year.

b) Incident Response
i) ESD shall:
(1) Develop and exercise documented incident handling and response procedures that specify when and how to escalate response. Make analysts aware of the procedures, and how to apply them. Utilizing these procedures, maintain a 24x7 incident/event handling capability and recommend actions to the partner to be taken in response to an on-going or post-discovery incident. This may include port or protocol blocks or other actions.
(2) Utilize a robust, automated tool such as Remedy, or a COTS product.
(3) Review and distribute updated incident response guidelines, checklists and recommended procedures at least annually.
(4) Maintain an incident/event handling operations Master Station Log. Entries shall be kept up-to-date and complete.
ii) The partner shall:
(1) Develop a program to allow for proper incident handling and response. Provide follow up and feedback to DISA on the recommended actions.
(2) Track incidents, support the response process and generate managerial reports.

(3) Obtain and maintain active SIPR accounts for sufficient technical and managerial personnel to cover the potential for 24x7 incident response via classified means. Develop formal personnel recall procedures to support timely incident response. Provide the POC information to DISA for the 24x7 personnel DISA can contact to initiate and manage incident response actions as required.

c) Incident Response – Analysis

i) ESD shall:

(1) Provide analysis of incidents in accordance with documented policies and procedures that incorporate methods to determine the threat, risk or damage an incident may impose on partner networks. The analysis shall be based on (1) any similar events or activities in Theater and/or across the DoD networks, and/or (2) current attack or malicious code information. DISA shall collaborate with United States Strategic Communications (USSTRATCOM) Joint Chiefs Operations (J3) and Joint Chiefs Intelligence (J2) analysts and service CNDSP peers as appropriate.

(2) Utilize drill-down capabilities into HBSS Enterprise Policy Orchestrator (ePO) server to provide enhanced host-based analysis.

(3) Maintain a list of POCs and phone numbers of CND technical experts in other DoD agencies and commercial organizations that can give advice and information. Update list at least every six (6) months.

(4) Operate on a 24x7 basis. Does not require a recall roster, but plans and procedures must be in place to augment existing personnel to surge operations in response to a major incident, and maintain operations for a period of at least 14 calendar days.

ii) The partner shall:

(1) Acknowledge, maintain and reference all post-incident analysis disseminated by DISA or other sources. Provide any applicable follow up and timely feedback to this analysis.

(2) Acknowledge, maintain and reference any trend analysis on incident data disseminated by DISA or other sources to identify common vulnerabilities, and develop countermeasures and mitigation strategies.

4) Sustain

a) Sustainment Activities

i) ESD shall:

(1) Ensure that vendor maintenance, support, and licensing are current and maintained throughout the sensor lifecycle.

(2) Provide sustainment and configuration management services for all sensors, to include baseline C&A.

ii) The partner shall:

(1) Maintain updated copies of all CNDSP Memorandums of Understanding (MOUs), Memorandums of Agreement (MOAs), SLAs, or other contracts with all CNDSP providers and provide these documents to DISA to ensure situational awareness of any other CNDSP alignments.

(2) Maintain awareness of the requirement to notify DISA of any changes to network security configurations, and provide advance notification to DISA of any

scheduled maintenance on network assets, power outages and other activities that may affect CNDSP operations.

Appendix D – Inherited Information Assurance Controls

ESD has documented the following Inherited IA Controls in accordance with the DoD IA Certification and Accreditation Process (DIACAP):

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

Control	Control Name	Description	Supporting Rational
DCSP-1	Security Support Structure Partitioning	The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (i.e. 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 Invoice Account Code (IAC).
EBBD-1	Boundary Defense	Boundary defense mechanisms, to include firewalls and network Intrusion Detection Systems (IDS), are deployed at the enclave boundary to the WAN. Internet access is permitted from a demilitarized zone (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 ISs by physical or technical means.	The enterprise is responsible for the boundary defense mechanisms and IDS system deployment. This cannot be accomplished by a system within the enterprise.

Control	Control Name	Description	Supporting Rational
EBBD-3	Boundary Defense	Boundary defense mechanisms, to include firewalls and network IDS, are deployed at the enclave boundary to the WAN and at layered or internal enclave boundaries and key points in the network as required. All Internet access is prohibited.	The enterprise is responsible for the boundary defense mechanisms and IDS system deployment. This cannot be accomplished by a system within the enterprise.
EBPW-1	Public WAN Connection	Connections between DoD enclaves and the Internet or other public or commercial WANs require a DMZ.	Connections of enclaves and the internet or other public or commercial WANs is the responsibility of the enterprise. This control cannot be accomplished by a system within the enterprise.
EBVC-1	Virtual Private Network (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 ISs. Both inbound and outbound public service IM traffic is blocked at the enclave boundary. *NOTE: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.*	Blocking of the inbound and outbound traffic is the responsibility of the enterprise and this control cannot be accomplished by a system within the enterprise.

Control	Control Name	Description	Supporting Rational
ECND-1	Network Device Controls	An effective network device control program (i.e. routers, switches, and 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 (i.e. an information assurance vulnerability alert (IAVA).	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
ECND-2	Network Device Controls	An effective network device control program (i.e. routers, switches, and 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 (i.e. IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
PECF-1	Access to Computing Facilities	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.	Ensuring only authorized personnel are granted access to a site is the responsibility of the site. A system cannot satisfy this requirement.

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

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

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

Appendix E – Acronyms

The following acronyms are referenced throughout this T&C.

Acronym	Definition
AIS	Automated Information System
AOR	Area of Responsibility
ASC	Application System Code
ASI	Automated System Interruption
AS&W	Attack Sensing and Warning
ATC	Authority to Connect
ATO	Authorization to Operate
BAN	Billing Account Number
BCP	Business Continuity Plan
BDC	Backup Domain Controller
BETC	Business Event Type Code
BMMP	Business Management Modernization Program
BOM	Bill of Materials
BPN	Business Partner Network
BTA	Business Transformation Agency
CA	Certification Authority
C&A	Certification and Accreditation
CAP	Connection Approval Process
CAR	Customer Account Representative
CCAO	Classified Connection Approval Office
CCC	Central Communications Center
CCER	CENTRIXS Cross Enclave Requirement
CD2	Customer Management Division
CENTRIXS	Combined Enterprise Regional Information Exchange System
CERT	Certification
CFO	Chief Financial Officer
CIC	Customer Identification Code

Acronym	Definition
CII	Classified Information Incidents
CIO	Chief Information Officer
CIS	Centralized Invoice System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CL	Confidentiality Level
CME	Customer Management Executive
CMI	Classified Message Incident
CNC	Coalition NetOps Center
CND	Computer Network Defense
CNDS	Computer Network Defense Service
CNDSP	Computer Network Defense Service Provider
COA	Course of Action
COLL	Collection
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CP	Content Provider
CPU	Central Processing Unit
CTNOSC	CONUS Theater NetOps and Security Center
CTO	Chief Technology Officer
DAA	Designated Approving Authority
DBSMC	Defense Business Systems Management Committee
DCC	DISA Command Center
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISB	Disbursement
DISR	DoD Information Technology Standards Registry
DRS	Dynamic Resource Scheduling

Acronym	Definition
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITPR	DoD Information Technology Portfolio Repository
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DPAS	Defense Property Accountability System
DSD	Data System Designator
EBN	Enterprise Backup Network
ECA	Enclave Connection Authority
ECA	External Certificate Authority
ELO	External Liaison Officer
eMASS	Enterprise Mission Assurance Support Service
ePO	Enterprise Policy Orchestrator
ESD	Enterprise Services Directorate
ESD-NA	Enterprise Services Directorate – Network Assurance
EULA	End User License Agreement
FAQ	Frequently Asked Question
FC	Fibre Channel
FISMA	Federal Information Security Management Act
FMLO	Financial Management Liaison Office
FOC	Full Operational Capability
FRS	Financial Reporting System
FSO	Field Security Operations
FY	Fiscal Year
GAO	General Accounting Office
GIAP	GIG Information Assurance Portfolio

Acronym	Definition
GNSC	Global NetOps Support Center
GOTS	Government Off-the-Shelf
HA	High Availability
HBA	Host Bus Adapter
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
IA	Information Assurance
IAC	Invoice Account Code
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATO	Interim Authorization to Operate
IATT	Interim Authority To Test
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IBE	Initial Business Estimate
IDS	Intrusion Detection System
IECA	Interim Enclave Connection Authority
IFAS	Industrial Fund Accounting System
IM	Instant Messaging
INFOCON	Information Operations Condition
I/O	Input/Output
IOC	Initial Operational Capability
IOE	Initial Operating Environment
IP	Internet Protocol
IPC	Interim Production Connection
IPS	Intrusion Prevention System
IPAC	Intra-Governmental Payment and Collection System
IRB	Investment Review Board
IRRT	Incident Readiness Response Team
IS	Information System

Acronym	Definition
IT	Information Technology
I&W	Indications and Warning
J2	Joint Chiefs Intelligence
J3	Joint Chiefs Operations
JCD	Joint CERT Database
JTA	Joint Technical Architectural
JTF-GNO	Joint Task Force – Global Network Operations
KO	Contracting Officer
LE	Letter Estimate
LECA	Local External Certification Authority
LIECA	Local Interim External Certification Authority
MAC	Mission Assurance Category
MIAG	Mandatory IA Guidance
MIPR	Military Interdepartmental Purchase Request
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAS	Network Attached Storage
NAT	Network Address Translation
NDAA	National Defense Authorization Act
NetOps	Network Operations
NIST	National Institute of Standards and Technology
OE	Operating Environment
OMB	Office of Management and Budget
OOB	Out-of-Band
OS	Operating System
OSD	Office of the Secretary of Defense
OUSD	Office of the Under Secretary of Defense
PDC	Primary Domain Controller
PE	Planning Estimate
PIN	Personal Identification Number

Acronym	Definition
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPSM	Ports, Protocols and Services Management
RACE	Rapid Access Computing Environment
RISC	Reduced Instruction Set Computing
SA	System Administrator
SAN	Storage Area Network
SEA	Server Enterprise Architecture
SEA	Storage Enterprise Architecture
SIP	Service Improvement Plan
SIPRNet	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SMC	Systems Management Center
SRF	Service Request Form
STIG	Security Technical Implementation Guide
STE	Secure Telephone Equipment
ST&E	Security Test and Evaluation
T&C	Terms and Conditions
T&D	Test and Development
TAS	Treasury Account Symbol
TNC	Theater NetOps Center
TPN	Trading Partner Number
TRO	Targeted Response Option
UCAO	Unclassified Connection Approval Office
USC	United States Code
VA	Vulnerability Assessment
VAA	Vulnerability Analysis and Assessment

Acronym	Definition
VM	Virtual Machine
VMS	Vulnerability Management System
VPN	Virtual Private Network
WAN	Wide Area Network
WCF	Working Capital Funds

Appendix F – Glossary

Term	Description
Accreditation	Formal declaration by a DAA that an IS is given approval to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (DoDI 8510.01)
Authorization to Operate (ATO)	Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years. (DoDI 8510.01)
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 partner. Detailed charge information supporting the bill can be found on the invoice available via 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.
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. (DoDI 8510.01)
Charges	Amount the partner is required to pay for the services provided.
Confidentiality Level (CL)	Determined by whether the system processes classified, sensitive, or public information.
Customer Account Representative (CAR)	A representative of ESD who serves as the primary POC to the partner for ESD services. The CAR is responsible for ensuring the partner is satisfied with ESD services.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. (DoD 8510.01)

Term	Description
DoD Components	The United States Deputy Secretary of Defense (and all sub-components), the Military Departments, and the Joint Chiefs of Staff
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.
Enclave Connection Authority (ECA)	Authority to connect a device/asset to the ESD networks granted by process compliance for interim connections and granted by the managing ESD designated official for full production activity.
Exceptions to Normal Processing	Temporary requirements that cannot be accommodated within agreed-to levels of services or customary procedures.
External Certificate Authority (ECA) Program	The DoD has established the ECA program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD ISs. The DoD Public Key Infrastructure (PKI) Program Management Office (PMO) has designated the ECA External Liaison Officer (ELO) as the single POC to receive and coordinate all communications between the ECA community, DoD programs, and the DoD PKI PMO.
Full Operational Capability (FOC)	A system is declared FOC when it has been migrated into ESD service and has executed its function for the agreed-to period (30 days after IOC declaration) without critical or high incidents, and it has completed all other defined exit criteria.
In-Cycle Changes	Refers to permanent changes to workload estimates or technical requirements occurring during the term of the SLA.
Initial Operational Capability (IOC)	A system reaches IOC when the application has been loaded, tested, and opened to the user base for production.

Term	Description
Initial Operating Environment (IOE)	A system reaches IOE when accepted proposals/LEs have IT assets that have progressed successfully through implementation and have been turned over to the partner to load their application(s) and data.
Interim Authorization to Operate (IATO)	A temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.
Interim Enclave Connection Authority (IECA)	Connection authority granted for device interim connections to the ESD Out-of-Band Network (OOB) and EBN in order to complete compliance.
Interim Production Connection (IPC)	Certain systems require connection to the production network for OS and software installation. This connectivity is limited to the site and traffic will be blocked to wide area networks (WANs). Site IAM will acknowledge requirement for IPC and that status will be reflected in the documentation provided for Local Interim External Certification Authority (LIECA). Central Communications Center (CCC) will review the documented IPC requirement prior to activating production ports under LIECA connection status. Documentation for this process includes a justification/explanation of the requirement and validation through the site IAM/IAO.
Invoice	A detailed listing of the type and quantity of services used by the partner for the period of time indicated, and the related charge to the partner for those services.
Letter Estimate (LE)	An LE is a formal document submitted to the partner as a result of a request for new, or changes to existing, workload. The LE restates the partner's expectations/mission, requirements, assumptions, and the recommended technical solution. It also includes the estimated cost for implementation and sustainment of the new or changed workload. LEs establish the basis for, or changes to, the SLA.
Local External Certification Authority (LECA)	LECA is the final network connection approval required before a device can be connected to the ESD production network accessible to WANs. Mandatory IA Guidance (MIAG) criteria compliance has been demonstrated to the approval authority and connection approval has been granted. Local Authority to Connect (ATC) is differentiated from ATC as is described in DISA Connection Approval Process (CAP) documents, and in this document only applies to ESD internal processes. The MIAG contains the complete list of documentation required to be submitted to the approving authority for approval.

Term	Description
Local Interim External Certification Authority (LIECA)	LIECA is the connection status assumed by a device as it is being prepared for production network connection. MIAG criteria are applied to the device as is applicable for 'interim' connection to the OOB, EBN, and in special cases, limited production network access. LIECA is differentiated from IECA as is described in DISA CAP documents, and in this document only applies to ESD internal processes. For this process, the required documentation is an email that contains the following information: • device name • IP address of the new device • hosting site • managing site • connection type requested IAM/IAO notification should also be included in the process.
Modification/Amendment	A modification or amendment 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, or amendments to, the SLA may be requested by either party and must be in writing. These changes require the approval of both parties and should have sufficient lead-time to permit appropriate resource adjustments to be made. Negotiations shall be between the ESD and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA shall remain in effect. *NOTE: For small modifications such as POC updates, formal approval is not necessary but all parties shall be informed of the change.*
Operating Environment (OE)	The OS on the server, i.e. Windows, Linux or UNIX
Partner	The Service or Agency for which ESD provides services.
Planning Estimate (PE)	An estimated project cost for sustainment of services provided to the partner each FY (Oct – Sept).

Term	Description
Renewal	The partner and ESD shall review the SLA annually, and as required, to determine if modifications or amendments are needed to reflect the partner's support requirements for the next FY, and to accurately reflect any changes to operational policy. The PEs shall be renewed no less than annually and shall be reconciled to the SLA as part of an annual SLA review. Negotiations shall be between the ESD and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA shall remain in effect indefinitely.
Service Catalog	Provides descriptions of each service DISA offers, as well as services being developed in the pipeline.
Service Level Agreement (SLA)	A formal agreement documenting the services that ESD provides to the DoD Service and Agency partner.
The Agreement	The provisions set forth in the SLA, PE, Service Catalog, and T&C, together with all modifications and amendments that constitute the entire agreement between ESD and the ESD partner.

Appendix G – References

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

1) CJCS Instruction 6510.01F, Information Assurance and Computer Network Defense, February 2011
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

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

3) DoD Directive (DoDD) 8500.01E, Information Assurance, April 2007
http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

4) DoD Financial Management Regulation 7000.14-R, January 2012
http://www.defenselink.mil/comptroller/fmr/

5) DoD Financial Management Regulation 7000.14-R, Volume 11B, Reimbursable Operations, Policy and Procedures – Working Capital Funds (WCF), December 2010
http://www.defenselink.mil/comptroller/fmr/11b/index.html

6) DoDI 4000.19, Interservice and Intragovernmental Support, August 1995
http://www.dtic.mil/whs/directives/corres/pdf/400019p.pdf

7) DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, June 2011
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

8) DoDI 8500.2, Information Assurance Implementation, February 2003
http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

9) DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 2007
http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

10) DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), August 2004
http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

11) DoD JTA Volume I, Version 6.0, October 2003
http://www.acq.osd.mil/osjtf/pdf/jta-vol-I.pdf

12) Federal Information Security Management Act (FISMA)
http://iase.disa.mil/fisma/index.html

13) GAO Information Technology – A Framework for Assessing and Improving Enterprise Architecture Management, Version 1.1, GAO-03-584G, April 2003
http://www.gao.gov/new.items/d03584g.pdf

14) National Defense Authorization Act (NDAA) for FY 2005, May 2004
http://www.cbo.gov/ftpdocs/54xx/doc5473/s2400.pdf

15) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, August 2009
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

16) Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, February 1996
http://www.whitehouse.gov/omb/circulars_a130

17) Public Law 107-347, E-Government Act of 2002, December 2002
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

18) USC, Title 10, Subtitle A, Part I, Chapter 7, Section 186, Defense Business System Management Committee, January 2012
http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t09t12+153+0++%28Defense%20B

19) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2208, Working-Capital Funds, January 2012
http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t09t12+1375+0++%28%29%20%20A

20) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2222, Defense Business Systems: Architecture, Accountability, and Modernization, January 2012
http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t09t12+1390+0++%28%29%20%20A

Document Source

1) All DoD Issuances
http://www.dtic.mil/whs/directives/

2) All OMB Circulars
http://www.whitehouse.gov/omb/circulars/#numerical

Appendix H – Performance Standards

These performance standards are available to all ESD partners.

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

Service	Service Objective	Service Description
Interactive Availability	98.5 percent availability	Portion of network/system controlled by ESD available to the partner during the interactive window.
Batch Throughput (mainframe)	95 percent or better completion rate and delivery	Completion rate and delivery by specified time during the batch window specified in the service level agreement (SLA). Partner initiated batch-processing outside the batch window will be processed as resources permit.
Job Failure Notification	Within 30 minutes	During normal working hours. Notification will be made after duty hours as requested by the partner.
Data Retrieval Services	15 Minutes 4 Hours 36 Hours	Tape, on-site (mount) Tape, off-site (local) Tape, off-site (backup site)
Server Capacity Utilization Reports	Monthly	Provides previous month's capacity utilization reports for 1) most ESD-provided server hardware, and 2) partner-provided server hardware for which the partner is paying Hardware Services.
Centralized Invoice System (CIS)	Bi-weekly	Billing amounts charged to Military Interdepartmental Purchase Requests (MIPRs) at the service level.

ESD also now offers System Network Availability Performance Service (SyNAPS) as an end-to-end monitoring tool to enhance the currently available performance monitoring tools. Please visit http://disa.mil/Services/Computing/Application-Monitoring/SyNAPS for additional information.

Appendix I – GCDS Performance Standards/Responsibilities

The following performance standards and responsibilities pertain only to partners utilizing the Global Content Delivery Service (GCDS).

DISA ESD:

1) Will provide immediate failover to a redundant GCDS node for disaster recovery
2) Will provide GISMC (Tier 0) response to the partner issue within two hours of receipt
3) Will provide triaged (Tier 1 or 2) response of the partner issue within 24 hours
4) Will provide a quarterly evaluation of partner usage and performance
5) Will notify the partner if the portal requires maintenance 72 hours prior to the maintenance event
6) Will provide log delivery and accessibility for 30 days on GCDS (the partner must enable)
7) Will allocate one SyNAPS transaction per URL integrated into GCDS. If multiple URLs are integrated under one Content Provider (CP) code, that counts as one URL. This normally occurs when many URLs are under sub-elements of the same domain.
8) Will allocate NetStorage space for a partner-designed apology page that will be displayed should the origin web server be unavailable. Once the GCDS network recognizes the web server is available, the apology page will revert to the partner's site.
9) Is not responsible for the content, look, and feel of the website and/or the partner apology page
10) Is not responsible for broken links on a website or failure of pages or graphics to load on the page
11) Will monitor the integrated URLs accessibility, performance, and status 24x7/365 on both the NIPRNet and SIPRNet
12) Will notify the partner immediately if there is a technical issue related to their application
13) Will notify the partner if the NetStorage allocation is reaching capacity
14) Will decommission an integrated URL 30 days following a partner's decommission action
15) GCDS will ensure the partner's URLs are available to their end users 99.9% of the time. The variable in this assessment is if the origin server is disconnected or no-longer operational. In this instance, DISA ESD will ensure an apology page created by the partner is displayed until the origin server is re-connected or is operational again.
16) GCDS will ensure the partner's performance metric interface, the GCDS Portal, is available to the partner 100% of the time.
17) GCDS will provide updates to the GCDS partners via the GCDS website at http://www.disa.mil/Services/Enterprise-Services/Infrastructure/GCDS
18) GCDS will not decommission a URL without the partner's written consent
19) GCDS will not troubleshoot an application if the triage does not indicate it is a GCDS problem

20) GCDS will not continue integration if all 125 hours per URL are used up during the integration process

21) GCDS will not re-integrate a URL if the partner has decommissioned the URL from GCDS and the URL was decommissioned from GCDS

22) DISA ESD will not refund integration costs if the URL has gone live on GCDS

DISA ESD Partner:

1) Will notify the appropriate DISA ESD CME team in writing of their intent to decommission two weeks prior to decommission

2) Will enable log storage on GCDS through the GCDS portal (part of the integration process)

3) The partner has the ability to store their logs in GCDS NetStorage indefinitely. Should this occur, the partner is responsible for overwriting their logs and the specified retention or cut-off point.

4) Has the flexibility to purge an event or the entire content. If the file is purged by accident, the partner must notify GCDS via the GISMC (Email: disa.columbus.esd.mbx.gcds-columbus@mail.mil) to attempt to recover the file.

5) If the partner's entire content is purged intentionally or accidentally, the partner understands that the data is unavailable to the end users until the propagation from the origin server is completed across the GCDS network

6) The GCDS integration team will make quarterly recommendations to the partner at no cost to enhance the performance of the application. The partner is under no obligation to accept these recommendations.

7) Must provide written consent to GCDS should they wish to decommission a URL

8) Has the flexibility to decommission a URL. If this occurs, the partner understands that the URL will be decommissioned from GCDS 30 calendar days from decommission. Once the URL is decommissioned, integration back into GCDS is considered a new integration costing $40K per URL (no-recurring cost). It is strongly suggested the GCDS PMO is notified at disa.meade.esd.list.gcds@mail.mil prior to taking such action.

9) Will inform the GCDS PMO anytime a POC responsible for the management of the integrated application changes

10) Is responsible for maintaining the allocation if the partner utilizes GCDS NetStorage

11) Is responsible for ensuring the IA accreditation of the application is maintained. If the accreditation expires, the partner must notify the GCDS PMO immediately to suspend content delivery until the application is re-accredited.

12) Understands if their URL(s) transitioned to GCDS from DISA NCES in FY10, their content delivery continued without interruption. There was no cost associated with this transition.

13) Understands if they were brought onto GCDS with an LE, the recurring billing for GCDS stopped on 1 October 2012 due to the GCDS transition to the DISN Subscription Service (DSS)