Defense Information Systems Agency

A Combat Support Agency

Defense Information Systems Agency

Terms and Conditions

Applicable to all Service Level Agreements

Published Date:
October 2016

Version 6.1

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	Sect 6; Appendices G,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	Sect 5,10; Appendices E,F,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 H (previously I) – GCDS Performance Stds / Responsibilities
5/2013	4.3	Sect 1-7,10; Appendices A-C,E	ES244	Added info re: socializing changes to the agreement with the partner; moved IOE, IOC, and FOC definitions from 5.0 to 2.0 (first instance of usage); clarified timing guidance for completing the draft/final SLA; added FISMA reporting info; updated IRB website URL; added statement re: partner PM IA duties; other standard changes
7/2013	4.4	Sect 2; Appendices B,I	ES244	Added note to Sect 2 re: partner program &financial mgrs; added Vendor POC row to SW Transfer form; updated GCDS Perf Stds
10/2013	4.5	Sect 8-10; Appendices C,G	ES244, ES535	Added verbiage re: A-goal & C-goal pricing in Sect 2; added communications input in sect 8; revised references to IA Architecture and updated them to DOD DMZ Extension; changed verbiage re: partner-owned HW in Sect 9; revised DMZ verbiage & added VMS link in sect 10; corrected Combatant Command acronym in App C; updated references in App G
3/2014	4.6	Sect 1,9,10; Appendices A,B; All	ES454	Removed statement re: DODI 4000.19 in Sect1, #1 and Sect.7, #2; added verbiage re: partner-owned HW to Sect 9 (para 4-7); updated information re: classified info spillages in Sect 10 (#9); added Termination Worksheet and SW Transfer Agreement forms as attachments to this doc; changed Enterprise Services Directorate/ESD to Enterprise Information Services/EIS
4/2014	4.6.1	Sect 4,5,7,10; Appendices E,G,H	ES454	Changed IOE to IOC for SLA creation; corrected FMLO email; replaced FRS with DCAS; added note that SIPRNet link won't work unless on SIPRNet; updated links in References; corrected SyNAPS link

Date	Version Number	Section Reference	Changed By	Description
6/2014	4.7	Sect 2,8	ES454	Added Sect 2, Onboarding Paths; added clarifying verbiage to Sect 8, Duration and Termination of Agreement
12/2014	4.8	All	ES454/ SI81	Changed EIS to DISA, font from TNR to Arial; removed Appendix D – Inherited IA Controls and added all IA Control documents as attachments; added milCloud and milCloud Plus info to Sects 2, 3, 6, & 11; added info on C&A expiration process to Sect 4, req'd MIPR details to Sect 6, new guidelines on partner response times to annual reviews and re-signatures of new / existing SLAs to Sect 8, verbiage that addresses partner application SW to Sect 8, security updates to Sect 11, audit request info to Sect 12; updated server HW in Sect 10; updated References and Perf Stds appendices
10/2015	5.0	All	BDM52	Changed the cover, header, and p1 from DISA EIS T&C to DISA T&C based on DISA reorg; additional verbiage/clarification on change requests (Sect4, #7); additional verbiage/clarification on workload history for estimate creation (Sect4,#11); additional HW/OS listed and z/Linux info (Sect9,#2,a); added ex of comm networks (Sect9,#2,c); added CoN info and reference (Sect11,#1,c & App F); spelled out all instances of IS (information system); updated JTF-GNO to USCYBERCOM; made grammatical corrections throughout; removed references to SyNAPS; changed the terms Classified Information Spillage (CIS) and Classified Messaging Incident (CMI) to Negligent Discharge of Classified Information (NDCI) per SecDef memo; changed "CME" to "Engagement Executive throughout; updated GCDS Perf Stds/Responsibilities (App H); added note for clarity to Sect6,#2,b; updated CNDSP (App C); updated acronyms & references; added Audit info (App I); updated IA control docs; added verbiage re: CALs; replaced VMS w/ CMRS
11/2015	5.0.1	Appendix C	BDM52	Added 2 clarifying paragraphs and COLS-NA acronym to the beginning of the CND appendix

Date	Version Number	Section Reference	Changed By	Description
3/2016	5.1	Throughout	BMD52	Added info re: RRP (Sect1&3.d); adjusted verbiage to clarify partner and DISA responsibilities upon partner acceptance of LE and DISA acceptance of MIPR(Sect6); adjusted “Duration” wording to comply with DODI 4000.19 (Sect8); added/mod verbiage re: HW responsibilities (Sect10#2); replaced old terms Computer Network Defense (CND) and Cybersecurity Defense (CD) with new term Cyber Defense (CyDef) and CNDSP with CDSP (Sect11 &AppF); moved Acronym, Glossary, & References appendices to App A-C and adjusted subsequent appendices accordingly; updated App C Refs; added para 9 &10 to App F; added clarifying verbiage re: audit readiness, LEs, MOUs, and milCloud to App I; minor grammatical and format corrections (throughout)
8/2016	6.0	Throughout	BDM52	Made changes to Intro wording; moved 1st 10 items formerly under Mgmt Process Responsibilities to Add’l Responsibiliites and the remaining items (re: PEs) under Pricing; removed Termination Worksheet and SW Transfer Agreement appendics; moved Perf Stds, Audits, Cyber Def, and GCDS appendices into body of doc; removed service POC & descriptions from Cyber Def section; removed first paragraph (re: milCloud) from Onboarding Paths and Business Estimate Process sections; rewrote Cybersecurity section (formerly Security and Access); rewrote Audits section; added RMF and Audit controls as attachments; moved BMMP info to Add’l Responsibilities sect & deleted BMMP sect; made updates and additions to gloassary; made minor grammatical and formatting changes; made other updates to content throughout . Note: If you wish to view all changes in detail, please send a request for the track changed copy to disa.denver.esd.mbx.e2ecrmchangemanagementrequest@mail.mil
10/2016	6.1	Sect 7, 9; Appendix B	BDM52	Made minor updates to Cybersecurity (Sect9); removed old terms from Glossary (AppB); updated comm verbiage (Sect7,para1.c) Note: If you wish to view all changes in detail, please send a request for the track changed copy to disa.denver.esd.mbx.e2ecrmchangemanagementrequest@mail.mil

Table of Contents

1.0 Introduction

The Terms and Conditions (T&C) constitutes the policies, roles, and responsibilities of the Defense Information Systems Agency (DISA) overarching agreement with all Department of Defense (DOD) Service and Agency mission partners for whom DISA provides Computing services; Enterprise Application and Identity and Access Management (IdAM) services; Cyber Compliance and Cybersecurity services; and the Global Content Delivery Service (GCDS). As multiple directorates within DISA perform the roles and responsibilities involved in providing these services to the mission partners, any DISA entity involved in the role of provider will hereinafter be referred to as “DISA.” The mission partner will hereinafter be referred to as “partner.” The whole of the parts that make up the overarching agreement between DISA and the partner will hereinafter be referred to as “the Agreement.” The Agreement is made up of the following:

1) Service Level Agreement (SLA) – documents the service(s) DISA provides to the partner. All services provided by DISA must be documented in an SLA. Stated service levels will 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 DISA.
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 DISA for the partner as a planning and budgeting tool for the services DISA provides.
3) Service Catalog – provides descriptions of each service DISA offers, as well as services being developed. DISA will only provide those services advertised within the Service Catalog, and unless otherwise specified in the SLA, these services will be delivered as described in the Service Catalog.
4) T&C – constitutes the policies, roles, and responsibilities of DISA’s 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 will not be restated in the SLA.

For applicable Computing and Enterprise services*, 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.

**Applicable services: Mainframe Hosting; Server Hosting and Virtualization; milCloud Plus; DOD Automated Time, Attendance, and Production System (DATAAPS); DOD Enterprise Email (DEE); DOD Enterprise Portal Service (DEPS); and Global Content Delivery Service (GCDS).*

NOTE: Some changes to a partner’s existing Computing services workload can be accomplished through an expedited process without the need for an LE or change to the SLA.

Any change to the SLA, Service Catalog, or T&C that impacts the overall Agreement will be socialized with the partner by their respective Mission Partner Engagement Executive team.

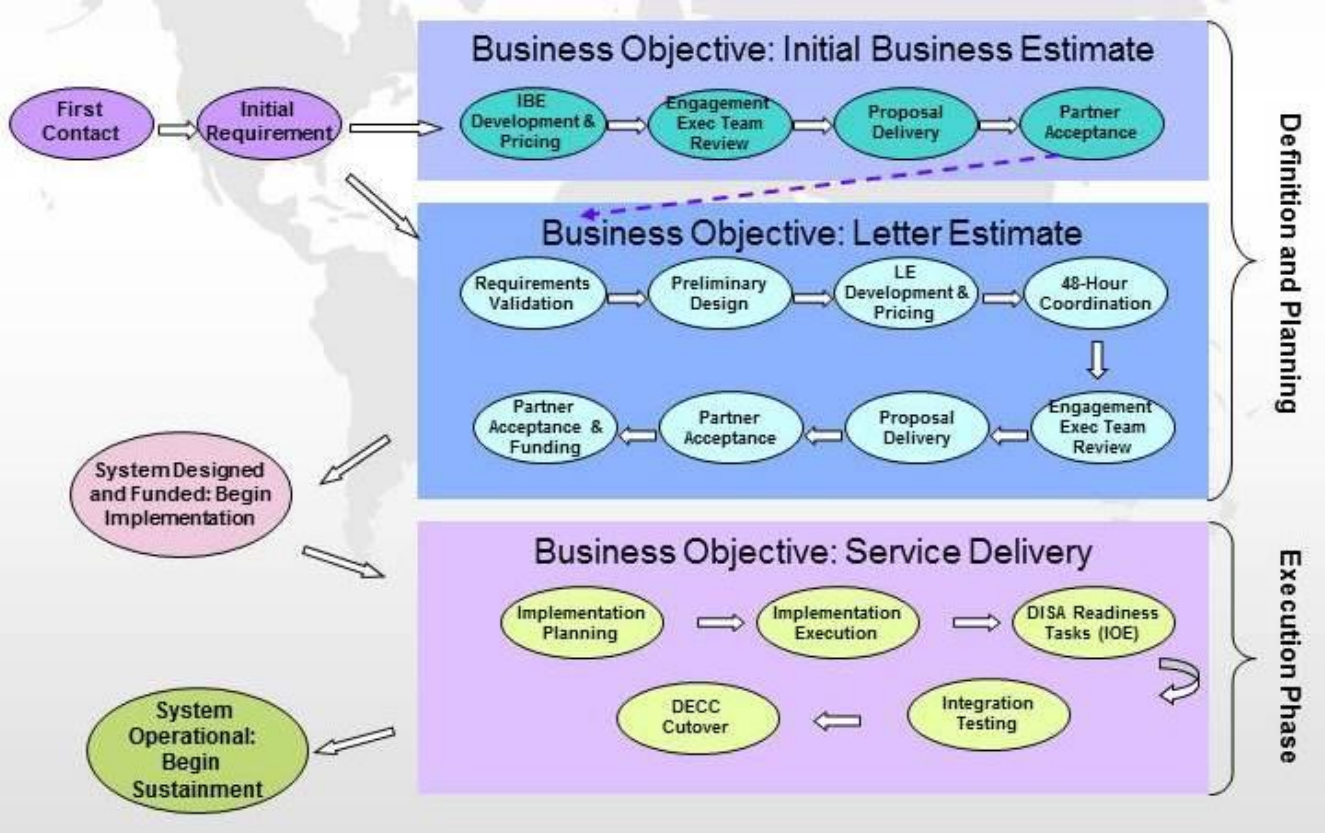
NOTE: milCloud Infrastructure as a Service (IaaS) does not require an LE, SLA, or PE and operates under its own terms and conditions. The full terms and conditions for milCloud IaaS self-service virtual data centers (VDCs) can be found by accessing the Cloud Services Marketplace at https://milcloud.mil.

2.0 Onboarding Paths

The End-to-End (E2E) fulfillment process governs the project workflow for new partner Computing and Enterprise Services workloads hosted by DISA and any changes to those workloads. The E2E process outlines the initiation, definition, planning, and execution of the technical projects that result from these hosted services.

1) Streamline Standard
    a) Streamlined engineering (only operating systems [OSs] supported by capacity services contracts and standard network architecture apply)
    b) Provisioning timelines vary per OS type specified
    c) No partner-provided network devices allowed
2) E2E Non-Standard (Custom)
    a) Complex engineering effort (may contain non-standard architecture)
    b) Provisioning timelines vary per solution design specified
3) milCloud Plus (DISA Engineered/Managed)
    a) Baseline/build documentation engineered by DISA
    b) Implementation by DISA
    c) Provisioned by a Defense Enterprise Computing Center (DECC) on behalf of the partner
    d) DISA-managed VDC
    e) milCloud optional services (e.g., system and database administration)

3.0 Business Estimate Process


First Contact
Initial Requirement
Business Objective: Initial Business Estimate
IBE Development & Pricing
Engagement Exec Team Review
Proposal Delivery
Partner Acceptance
Business Objective: Letter Estimate
Requirements Validation
Preliminary Design
LE Development & Pricing
48-Hour Coordination
Engagement Exec Team Review
Proposal Delivery
Partner Acceptance
Partner Acceptance & Funding
System Designed and Funded: Begin Implementation
Business Objective: Service Delivery
Implementation Planning
Implementation Execution
DISA Readiness Tasks (IOE)
Integration Testing
DECC Cutover
System Operational: Begin Sustainment
Definition and Planning
Execution Phase

While both Initial Business Estimates (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 business 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 10 business days following the agreement of baseline requirements.

1) Initial Business Estimate
    a) First Contact – Initial communication between the partner and DISA. 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.
    b) Initial Requirement – The DISA Engagement Executive 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 Engagement Executive) of ability to respond.

c) 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 (Office of the Secretary of Defense [OSD]-approved partner billing rate) and C-goal (reimbursable cost of services) service prices. Outcomes include an IBE, pricing entry, and a tracking system update.

d) Engagement Executive or Division Review – All IBEs shall be reviewed at the Engagement Executive-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.

e) 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.

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

2) Letter Estimate

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

b) Project Team and Partner Coordination – The DISA project lead and Information Assurance (IA) Technical Advisor work with the partner to attain in-depth system hosting requirements and address numerous issues including the partner's IA posture; network/communication considerations including the registration of ports (internal and external); the partner's integrated milestone schedule; and funding and resource availability. Outcomes include a tracking system update, completed SRF, creation of a solution document for LE development and pricing, Bill of Materials (BOM) initiation, IA risk assessment, and determination (with Engagement Executive) of DISA's ability to respond.

c) Solution Document Development – The DISA team (including appropriate engineering, capacity, operations, communications, IA, 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.

d) LE Development and Pricing – The development of the LE 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 document and a tracking system update.

e) 48-Hour Coordination for Non-Standard Projects – To ensure a formal proposal from DISA represents an accurate description and pricing of DISA services, coordination with DISA service and financial management teams is mandatory.

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

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

   h) Partner Acceptance – The partner wishing to accept the LE shall be informed that DISA 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.

3) Service Delivery – Upon partner acceptance and funding of an LE, DISA 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).

   a) 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 partners to load their application(s) and data.

   b) IOC – A system reaches IOC when the application has been loaded, tested, and opened to the user base for production.

   c) FOC – A system is declared FOC when it has been migrated into DISA service and has executed its function for the agreed-to period (30 calendar days after IOC declaration) without critical or high incidents, and it has completed all other defined exit criteria.

4) Resource Request Process (RRP) – The RRP establishes standard guidelines for expediently processing requests for changes to sustainment/production partner workload. This process may NOT be used for new partner workload. Partner workload is considered to be in a sustained/production status when a project reaches FOC. The RRP may only be used for partners that have the following modifications to existing workload in place at a DECC:

   a) Server storage change.

   b) DEPS storage change.

   c) Physical OE and virtual OE (VOE) configuration changes based on requests for re-provisioning, additional memory, or central processing units (CPUs).

      No change to the SLA will be required; however, the PE will need to be updated to reflect the new increase.

   d) Software change.

   e) Communication requests.

NOTE: The partner's program manager approving project SRFs and the partner's financial manager authorizing the obligation of funds must be government employees.

4.0 Pricing

The PE is created by DISA for the partner as a planning and budgeting tool for the services DISA provides.

1) The PE serves the following purposes:

   a) Sustainment of Existing Workload – DISA will provide the partner with a proposed PE no later than the third quarter of the current FY for the following FY. The PE is reviewed by the partner and DISA to confirm that it provides an accurate representation of support provided to the partner. The partner shall ensure DISA 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.

   b) New Workload or Changes to Existing Workload – Upon signature of an LE, the DISA Customer Account Representative (CAR) will begin creating an SLA for new workload or modifying an existing SLA. Within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. No later than FOC, the SLA must be bilaterally agreed upon and signed by the partner and applicable DISA representatives. If this modification requires additional funds for sustainment throughout the remainder of the current FY, DISA will update the existing PE to reflect the change in cost. The partner must submit funding for implementation costs prior to DISA 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.

2) New DISA partner – Upon signature of an LE, the partner must submit funding for implementation costs prior to DISA beginning implementation of the workload. The MIPR must provide funding to cover estimated charges for at least one quarter, with amendments executed prior to the start of each succeeding quarter.

3) The partner shall provide estimates of anticipated workloads with which DISA can develop a target budget amount for the PE. To aid in this estimate, DISA will provide workload history from DISA's billing system (currently the Centralized Invoice System [CIS]), where it is available.

   a) Workload Estimates

      i. DISA will provide the partner with actual mainframe and storage usage information, as well as server and server storage usage analysis being provided during the year. To develop meaningful projections, the partner and DISA must collaborate, as the partner is ultimately responsible for all mainframe and server projections.

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

      iii. The partner shall furnish DISA with projections of future workload levels and support requirements at the Customer Identification Code (CIC) and the Application System

Code (ASC) levels. These must reflect known or anticipated changes not less than 180 calendar days prior to the known change.

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

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, DISA, in conjunction with the partner, will adjust the services in the SLA accordingly, matching services to the partner funding level.

b) SLA Preparation

i. The SLA must be specific as to the types and levels of services required.

ii. The partner shall furnish the projected workload for DISA to effect the proper level of support.

iii. The SLA must contain any additional DISA and/or partner responsibilities that are consistent with the workload rights and support.

5.0 Funding and Billing

1) Funding – Signing the LE indicates the partner's intent to pursue the solution as documented. Upon acceptance of the MIPR, DISA becomes obligated to provide the services documented 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 must submit all MIPRs to the Financial Management Liaison Office (FMLO). The FMLO will submit a MIPR Acceptance Form (DD Form 448-2) to the partner acknowledging acceptance of the funds received.

   Within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. No later than FOC, the SLA must be bilaterally agreed upon and signed by the partner and applicable DISA representatives.

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

   - The LE number and funding source
   - The Treasury Account Symbol (TAS) for both trading partners (DISA and partner)
   - The Business Event Type Code (BETC) for both trading partners. DISA-issued MIPRs are "DISB" (disbursement) and received MIPRs are "COLL" (collection)
   - The effective date and duration of the Agreement, to include the expiration of the funding source
   - The method of payment
   - The Business Partner Network (BPN) number for both trading partners
   - The method and frequency of performance (revenue and expenses) reporting
   - If applicable, provisions for advance payments and method of liquidating such advances
   - The parties' rights to modify, cancel, or terminate the Agreement
   - Accounting/finance office point of contact (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.
   - An alternative Dispute Resolution clause
   - The SLA number assigned by DISA
   - Where practicable, the application and/or ASC (Block 9)

   MIPRs must also include the following minimum information in the MIPR Description field (Field 9b):

   - Dollar amount – Implementation: $XXX.XX

- Dollar amount - ¼ (3 months) Annualized Recurring: $XXX.XX
- Name, email, and phone number of partner financial POC
- Purpose and description of services being procured
- Trading Partner Number: DOD Activity Address Code (DODAAC)
- Project Tracking Number: XXXX
- Implementation Billing Account Number (BAN) Code: XXXXXX
- Recurring BAN Code: XXXXXX

If an Implementation MIPR is required, it must abide by the following Project Order guidelines in Field 9b:

- Include project name, DEPS number, and an adequate description of the environment to be implemented.
- Include the following statements in their entirety:
  - "This order is placed in accordance with the provisions of 41 U.S.C. 6307, as implemented by DOD regulation."
  - "This order is for an implementation; it is non-severable and serves a bona fide need during the FY the funds are obligated."
- To account for any possible schedule slippage, use 30 September YYYY for all work to be implemented by the end of the current FY; otherwise, please use applicable scheduled date.

Funding documents must be issued and addressed to:

DISA Enterprise Services – CFEB41/FMLO

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-fmlo.eis.mbx.pen-miprmail@mail.mil.
MIPR acceptance forms must be e-mailed to the MIPR originator/issuer.

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

The partner shall work with DISA 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 will be billed via the Defense Cash Accountability System (DCAS). All other partners will be billed via the Intra-Governmental Payment and Collection System (IPAC).

The partner shall promptly review the invoice, and notify DISA of any disputed billings. Subsequent partner billings will 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. DISA and the FMLO must receive this data at least 30 business days prior to the effective date. DISA will change the appropriate CIC upon receipt of the new information, and will document this information in the partner's SLA.

Server and Storage –

- 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 DISA has completed the initial system implementation (e.g., hardware installation; storage allocation; OS load; and hardening, to include, but not limited to, Security Requirements Guides (SRGs), Security Technical Implementation Guides [STIGs], IA Vulnerability Management [IAVM], 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.
- For OEs that have undergone a technical refresh, when the new hardware is declared IOE, DISA allows 30 calendar 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 will be billed.

  NOTE: The 30 day timeline is for rate-based standard workload only and cost reimbursable items will be handled on a case-by-case basis.
- milCloud & milCloud Plus pro-rate services on a 30-day basis allowing the partner to terminate services after a minimum of one month of service. Both services allow partners to increase or decrease CPUs, memory and storage resources, but users are billed at the highest resource use in a 30-day period.

6.0 Duration and Termination of Agreement

1) Duration – In compliance with Department of Defense Instruction (DODI) 4000.19, the SLA between DISA and the partner will have an expiration date not to exceed nine (9) years from the signature dates of both parties. Any agreement with a signature date by either party eight (8) years or older must be reviewed and reissued for new signatures.

   The SLA will be reviewed annually at a minimum, ensuring DISA 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 must 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. Partners have 30 days from contact with a CAR to respond to annual review requests – whether it is a request to review the SLA for needed changes or concur on any changes made by DISA. If no response is received from the partner within 30 calendar days of the CAR's request, the SLA will be fully accepted as written and annotated as such in the Annual Review table.

   For a new or existing SLA that requires new signatures, within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. The support and services represented and documented in the SLA are considered valid for 30 calendar days from the date of the last DISA representative's digital signature. If no correspondence or partner signature(s) are received within that time, the SLA will be considered fully accepted as written and annotated as such. Any subsequent changes will require the negotiation and preparation of a new document and re-signature from all parties.

2) Termination – DISA requires written notice 180 calendar days in advance of the partner terminating any services provided. DISA will 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 DOD Financial Management Regulation (FMR), Volume 11B, chapter 11, paragraph 110102.

   a) With assistance of the DISA CAR, the partner shall provide a completed Termination Worksheet if one of the following occurs:

      i. The partner is eliminating DISA support/entire SLA.

      ii. The partner is decommissioning an entire application/ASC.

   b) The Termination Worksheet is not needed, but the partner must still provide written notification (e.g., digitally signed e-mail) to DISA, if:

      i. The partner is discontinuing an existing optional service such as database administration or application support, but not all support for an application/system.

ii. The partner wants to de-install existing hardware, but not an entire suite of hardware or application/system. In this case the partner shall open a ticket with their supporting service desk and notify their CAR.

iii. The partner wants to de-install or discontinue use of existing reimbursable application software; software can be found on reimbursable tab of the PE.

NOTE: To access the Termination Worksheet for use, please click on the paperclip icon to the left and double click on the Termination Worksheet attachment. In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.

7.0 System Technology

1) System Architecture

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

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

   c) Communications –

   The DOD demilitarized zone (DMZ) effort is one of the many NIPRNet hardening initiatives established to protect the NIPRNet. The scope of the DOD DMZ effort is specifically to place priority on the protection of private DOD systems (accessible via the NIPRNet only) against attacks from the Internet by establishing DOD DMZs and migrating NIPRNet-hosted Internet-facing DOD services into DOD DMZs. The approach to meet this priority is to quarantine public-facing applications in order to protect them. Additionally, the DOD DMZs will build in protections to segregate restricted and unrestricted applications from the private applications.

   The DOD DMZ will host only Internet-facing DOD services and applications. These are the public services and applications that must be accessible from the Internet. The DOD DMZ will no longer host private NIPRNet-only servers and applications since these are the services and applications that must not be accessible from the Internet. The DOD DMZs will provide separation between the public and private servers by segmenting the public servers within the controlled environment of the DOD DMZ. Access to the private services and applications will be blocked in such a way that access directly from the Internet to these services and applications will not be possible.

   Architectures also exist which provide connectivity for management and replication of data for disaster recovery.

2) Configuration

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

      - Itanium-based servers from Hewlett-Packard (HP)
      - Power7-based servers and mainframe servers from IBM and Unisys
      - x86-based servers from HP
      - SPARC-based servers from Oracle

The capacity services contracts provide hardware and OSs that include HP Windows, HP UNIX, Sun Solaris, IBM AIX, SUSE Linux, Red Hat Linux, zOS, zVM, and Linux on System z (z/Linux) (SUSE & Red Hat).

DISA 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); Distributed Resource Scheduling (DRS), which is the capability to place up to 32 physical servers into a resource pool where workloads can use resources on the fly; and high availability 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, 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:

- Dedicated power. Power can be shut off to the partition without impacting any other partition.
- CPUs and memory are allocated to the partition based on hardware configuration and cannot be shared with another partition or be dynamically reallocated.
- All I/O devices are dedicated to the physical partition including Ethernet cards, Host Bus Adapter (HBAs), internal disk drives, and optical drives.
- May be configured as a single OS, or host multiple virtual OSs.

In the IBM z/Linux mainframe space, virtualization is accomplished with logical partitions (LPARs). LPARs are managed by an IBM processor resource/system manager (PR/SM) and can share I/O and CPUs, with dedicated memory to each LPAR. Each LPAR will host its own OS (zOS, zVM, z/Linux). zVM is also a virtualization environment that can act as a hypervisor for other OSs (zOS, zVM, z/Linux) running as separate OEs. zVM can virtualize hardware resources (CPU, I/O, memory) and can share with OEs within a given zVM. z/Linux OEs can host SUSE Linux and Red Hat Linux.

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.

- Disk is used to hold databases, data warehouses, and flat files where immediate access to the data is necessary.
- 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 Storage Area Network (SAN) consisting of fiber channel (FC) switches connecting servers to their storage devices at each processing location. However, in special cases, with associated documentation, DISA can deploy Network Attached Storage (NAS) solutions. The SAN provides all standard storage functionality such as mirroring, data replication, data snapshots, data archiving, and security protection. The SAN supports all platforms at the processing location and can expand or shrink to meet changing requirements. Storage devices on the SAN are low cost and highly reliable. Boot-from-SAN is the standard architecture for all DISA-hosted platforms. Internal storage is only provided with server installations as a last resort when absolutely necessary. This architecture provides redundancy and highly available OS partitions and reduces outage times due to internal disk failures.

DISA 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. DISA has an off-site tape storage contract for safe and efficient tape storage.

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.

c) Communications – The architecture is comprised of three standalone networks (production, out-of-band [OOB]/EBN, DMZ extension), each isolated from the others. Each network uses its own network space, virtual local area networks (VLANs), and access control.

   i. Production – This network provides user level access to the application. Depending on the classification of the application and server it resides on, it will either sit in the web DMZ extension architecture or the production architecture. All traffic traverses a firewall inbound and outbound. The firewall also acts as the aggregation point for web and non-web traffic. Connections are also able to be load-balanced to provide reduced processing overhead and greater availability.

      A test and development (T&D) architecture also exists as a subset of the production network. This architecture provides separation from production applications as dictated by the STIG. Provisions for T&D Zone A-D are available.

   ii. Data Replication – This network is comprised of point-to-point circuits between DECC or Core Data Center (CDC)/Enterprise Operations Center (EOC) locations. It provides secure, IP based network transport for SAN, mainframe, tape and host-based replication.

   iii. OOB – This is the dedicated management network. It uses encrypted connections (Secure Socket Layer [SSL] and Internet Protocol Security [IPSec]) between the user and the hosting site to provide management capability for servers, applications and network devices. It also provides transport of monitoring and reporting devices. The OOB virtual private network (VPN) will be used for application, database, web, OS, or security administrator duties for scanning, monitoring, management, and administrative functions IAW IAVM notifications, Common Vulnerabilities and Exposures (CVEs), SRGs, and STIGS.

8.0 Ownership and Licenses

1) Hardware – DISA has negotiated a series of indefinite-delivery/indefinite-quantity capacity services contracts to obtain Unisys and IBM mainframes and IBM Power servers, Oracle SPARC servers, HP Itanium servers, HP x86 servers, and communications hardware.

   DISA is responsible for all DISA-owned equipment within the DECC. Annual inventories include all equipment in the DECC; however, only the DISA-owned assets are reconciled. DISA manages, tracks, and maintains accountability for only DISA-owned equipment.

   When DISA provides a basic services package (composed of power, processing, storage, etc.) to the partner, the following activities are the responsibility of DISA:

   - Establishing and maintaining auditable accountable records in the Defense Property Accountability System (DPAS)
   - Capitalizing and depreciating assets requiring capitalization
   - Maintaining supporting documentation
   - Hand receipting
   - Performing annual physical inventories and reconciliations

   Maintenance Support – DISA requires a standard level of maintenance support for all assets owned and maintained by DISA.

   If the information system is operating under Risk Management Framework (RMF), maintenance support is based on RMF system categorization. The organization being inspected/assessed obtains maintenance support and/or spare parts for information system components defined in maintenance control 6 (MA-6), control correlation identifier (CCI) 2896 within 24 hours for Low and Moderate Availability or immediately upon failure for High Availability (DOD defined).

   If the information system is operating under DOD IA Certification and Accreditation Process (DIACAP), maintenance support is based on DIACAP Mission Assurance Category (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.

   Partner/Vendor-Owned Hardware Assets – DISA policy states DISA will no longer accept partner-owned equipment after the first of October, 2011. Partner-owned equipment currently residing in DECCs will be grandfathered until end-of-life and technical refresh.

   Partners with approved, grandfathered hardware are obligated to provide complete lists of all assets, including communications hardware. Lists must include the following information for each asset:

   - Make
   - Model
   - Serial Number

- Barcode
- Physical Location
- Maintenance Vendor Name
- Maintenance Help Desk Phone Number
- Indication of Existing Warranty or Maintenance Contract
- Maintenance Contract Number
- Level of Maintenance Purchased
- Period of Performance (POP) Dates

DISA will monitor warranty/maintenance contract expiration dates as well as End-of-Life (EOL) timeframes for the asset, and will notify partners in writing within 180 days of expiration. This contact will initiate discussion between DISA and the partner to determine one of the following methods for dealing with maintenance expiration:

- Partner intends to provide their own extended maintenance on the hardware
- Partner intends to provide their own technical refresh for the hardware that has reached EOL
- Partner requests DISA acquire the necessary hardware for technical refresh through capacity services contracts

DISA will only provide maintenance support for partner-owned assets when all of the following conditions are met:

- Current DISA contracted vendors are able to support the asset
- EOL dates for the asset are more than 18 months away
- Partner agrees to fund the annual maintenance costs documented in the DISA cost estimate (either LE or PE)
- Asset remains on DISA's maintenance contract for a minimum of 12 months

DISA 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. DISA will track partner/vendor-owned assets for contractual purposes only in the IT Service Management – Change Configuration, and Asset Management (ITSM-CCA) tool and will annually inventory partner/vendor-owned property. Partner/vendor property custodians may, upon request, obtain current partner/vendor-owned inventory reports.

2) Software – DISA will 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 the End User License Agreement (EULA). The partner is responsible for the license management, tracking, change 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 DISA. No executive software is permitted to operate on a DISA mainframe or server that is not DISA-owned.

a) Executive Software

    i) Scope – for purposes of DISA 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.

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

b) Application Software

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

    ii) Server – Any application software not bundled in the server rate will be directly charged to the partner.

c) Software Transfers

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

    ii) 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 licenses are transferable. Any fees associated with a contract/agency transfer will 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.

    iii) Client Access Licenses (CALs) – A CAL is a software license that allows end users to connect with server software to use the software's services and various applications. As such, CALs are considered application software, unless otherwise discussed or for solutions under our "As a Service" model, which are owned and maintained by the partner. For Enterprise Services, management of CALs will be addressed by the program management office (PMO) on a case-by-case basis.

    iv) If the partner provides their own software for transfer to DISA, the following guidelines are required to ensure 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 submitted to DISA.

NOTE: To access the Software Transfer Agreement form for use, please click on the paperclip icon to the left and double click on the Software Transfer Agreement attachment. In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.

(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 DISA.

(5) For software currently covered under a renewable maintenance contract, the partner shall notify the applicable DISA CAR to change the address for renewal notification.

9.0 Cybersecurity

1) Information systems are defined as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. This includes automated information system applications, facilities, enclaves, outsourced IT-based processes, and platforms. All DOD-owned and DOD-controlled information systems that receive, process, store, display, or transmit DOD information, regardless of classification or sensitivity, will be implemented and sustained IAW references listed in Appendix C – References.

2) These roles, responsibilities, and requirements apply to government and contractor program managers (PMs), system owners (SOs), information system security managers (ISSMs), information system security officers (ISSOs) and technical personnel.

3) Anything regarding cybersecurity that falls outside of the standard support documented below must be negotiated with DISA and documented in Section 8.0 of the partner's SLA. Additional costs to accommodate associated non-standard requirements could potentially initiate an LE and the need for additional funding from the partner.

4) DISA **Enterprise Services:** DISA will maintain the Cybersecurity program for information systems wholly owned and operated by DISA and offered as an Enterprise service (e.g., DEE). This includes security and protection from unauthorized or malicious activity, security scanning, reviews, assessments, compliance, validation, and authorizations.

5) DISA **milCloud Services**:

   a) DISA and partners shall comply with the DISA standard hosting T&Cs contained herein.

   b) Partners are responsible for additional activities contained in the milCloud VDC T&Cs located at https://milcloud.mil/session/vdcTerms and the VDC Hosting Policy located at https://milcloud.mil/documents/vdc/VDC_Hosting_Policy.pdf.

6) DISA **milCloud Plus Services:**

   a) DISA and partners shall comply with DISA standard hosting T&Cs contained herein.

   b) Partners are responsible for additional activities located at http://www.disa.mil/Computing/Cloud-Services/MilCloud-Plus and under the "Additional information" tab, to include, but not limited to: (1) obtaining and submitting certificate of risk acceptance (CORA) documentation; (2) obtaining an Authorization to Operate (ATO), Authorization to Operate with Conditions (ATOC), or Interim Authorization to Test (IATT) to enter DISA hosting environments; (3) completing Ports, Protocols, and Services Management (PPSM) requirements; and 4) maintaining the security posture of the VDC to include the security status for the VDC and any VM managed by DISA.

   NOTE: The partner's Authorizing Official (AO) is exclusively responsible for this activity.

7) DISA **Standard Hosting Services**:

   a) DISA and partners shall:

i) Maintain the physical, personnel, information security, information system security, communications security, cybersecurity and RMF programs IAW DOD and other proper regulations, directives, guidelines, and other proper authority.

ii) Ensure early integration of security requirements are considered and addressed as part of the system development life cycle (SDLC).

iii) Ensure information systems possess the utmost security and protection from unauthorized or malicious activity through the appropriate implementation of DOD, USCYBERCOM, JFHQ-DODIN, Joint Staff, DISA regulations, directives, guidelines, and other proper authority.

iv) Ensure information system compliance and security mechanisms are implemented, present and operational IAW DOD, USCYBERCOM, JFHQ-DODIN, Joint Staff, and DISA regulations, directives, guidelines, and other proper authority. This includes, but is not limited to, IAVM notifications (IA Vulnerability Alerts [IAVAs], IA Vulnerability Bulletins [IAVBs], and IA Vulnerability Technical Advisories [IAVTAs]), CVEs, SRGs, STIGS, security scans, reviews, and assessments.

v) Ensure non-compliant information systems and applications with IAVM (IAVA, IAVB, and IAVTA), CVE, SRG, STIG, security scan, review, and assessment open vulnerabilities are patched or have plan of action and milestones (POA&M) documented and approved.

vi) Comply with the Federal Information Security Management Act (FISMA) defined framework and support standards for managing information security. This includes, but is not limited to, inventory of information systems, categorization according to risk levels, security controls, risk assessments, RMF authorizations, and continuous monitoring.

vii) Ensure Cybersecurity Defense Service Providers (CDSPs) are in place for information systems.

viii) Ensure information is not introduced above the level of classification for which the information systems are authorized.

ix) Ensure a valid RMF information system ATO or IATT or valid DIACAP ATO, IATO, or IATT exists.

x) Operate only authorized information systems and applications.

xi) Comply with all authorization decisions, including Denial of Authorization to Operate (DATO), and enforce Authorization Termination Dates (ATDs).

xii) Use the DOD's official Knowledge Service portal (https://rmfks.osd.mil/login.htm) for RMF or DIACAP enterprise policy and implementation guidelines.

xiii) Transition to RMF IAW DODI 8510.01 Enclosure 8, Tables 2, 3 and 4.

xiv) Ensure information systems are registered and maintained within the DOD IT Portfolio Repository (DITPR), Department of the Navy (DON) Applications and Database Management System (DADMS).

xv) Verify information system ports, protocols and services (PPS) are acquired, developed, implemented, maintained, and registered in the PPSM central registry (https://pnp.cert.smil.mil [SIPR]).

xvi) Use the PPSM Category Assurance Lists (CALs) for risk management processes, development, deploying information systems, and configuring network security devices.

xvii) Ensure NIPRNet and SIPRNet information systems are registered and use Enterprise Mission Assurance Support Service (eMASS) for RMF processes and packages.

xviii) Ensure Joint Worldwide Intelligence Communications System (JWICS) information systems are registered and use Xacta for RMF processes and packages.

xix) Report, through the proper chain of command, incidents; intrusions; disruption of services; or other unauthorized activities (including insider threat) which threaten the security of information systems, DOD operations, or IT resources immediately upon discovery.

xx) Comply, protect, and validate Controlled Unclassified Information (CUI), personally identifiable information (PII), Health Insurance Portability and Accountability Act (HIPAA) information and Payment Card Industry (PCI) information based on applicable federal, departmental, and/or agency policies and guidelines.

b) DISA will:

i) Update and maintain valid authorization decisions signed by the DISA AO for DISA information systems and applications in implementation and sustainment.

ii) Use the DISA RMF community of interest (COI) portal as the enclave and information system security Tier 3 Security Control provider. The official site is https://disa.deps.mil/disa/cop/rmf/default.aspx.

iii) Identify infrastructure RMF common control providers (i.e., policy, facility, and network).

iv) Maintain the high level DISA Inheritable Policies (DIP) package for DOD and DISA.

v) Maintain DISA eMASS common control provider authorization boundaries for facility and network as defined below:

(1) Facility description: The facility authorization boundary is determined by the infrastructure required to operate in preparation of hosting information systems or networks within the facility (building, environmental, physical security, personnel security, support personnel). The facility authorization boundary does not include any hosted information systems or networks.

(2) Network description: The network authorization boundary includes network assets providing connection from Non-secure IP Router Network (NIPRNet) and Secure IP Router Network (SIPRNet) service delivery points (SDPs) to physical server connections and includes virtual network hardware not to conflict with other authorization boundaries. The network authorization

boundary includes all DECC facility Command Communications Service Designators (CCSDs) for NIPRNet and SIPRNet network access.

vi) Ensure facility and network common control providers and Confidentiality, Integrity, Availability (CIA) impact levels are at least maintained as listed in the tables below.

Facility	**NIPRNet**	**SIPRNet**
Confidentiality	High	High
Integrity	Moderate	Moderate
Availability	High	High

Network	**NIPRNet**	**SIPRNet**
Confidentiality	High	High
Integrity	High	High
Availability	High	High

vii) Publish policy, facility and network common control documentation.

NOTE: To access these RMF common control documents, please click on the paperclip icon to the left and double click on the attachment. In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.

viii) Grant access for inheritance from common control packages.

(1) Policy – DIP-RMF

(2) Facility – DECC "DECC Name" – RMF

Example: DECC Oklahoma City – RMF

(3) Network – Enterprise Infrastructure Backbone Network (EIBN)

ix) Prohibit retesting of common control provider results unless agreed upon by all parties through written correspondence.

x) Accept partner DIACAP packages until RMF packages are assessed and authorized based on transition timelines.

xi) Sustain DISA DIACAP packages until RMF packages are assessed and authorized.

xii) Provide DIACAP inherited IA controls based on information system MAC and confidentiality levels.

NOTE: To access these DIACAP IA control documents, please click on the paperclip icon to the left and double click on the attachment you would like to view. In order to view the paperclip icon, you may have to select "Trust

this Host" under the Options tab or "Enable All Features" in the pop-up banner.

xiii) Provide, upon request, DIACAP eMASS accreditation scorecard to the partner as proof of compliance and validation with security controls.

xiv) Prohibit retesting of DIACAP inherited IA controls unless agreed upon by all parties through written correspondence.

xv) Provide cyber engagement services for workloads located within DISA hosting environments.

xvi) Notify partners within 180 calendar days prior to authorization expiration dates and every 30 calendar days thereafter, until new authorization expiration dates are provided and updated decisions are received.

xvii) Escalate partner expired authorizations to the DISA AO.

xviii) Prohibit information systems, operating with an IATT, to be used for operational purposes.

xix) Apply information system/application security fixes and vendor-recommended software maintenance as directed and approved by the partner.

xx) Assist with Negligent Discharge of Classified Information (NDCI) (i.e., spillages) within DISA hosting environments and hold partner organizations responsible for spillages. In the case of NDCI, partners are financially liable and will be billed for accumulated restoration costs.

NOTE: The minimum amount charged to partners for DEE NDCIs is $2,500 per incident.

xxi) Establish connections between DOD enclaves and the Internet or other public or commercial wide area networks (WANs) IAW NIPRNet DOD DMZ policy requirements.

xxii) Employ DMZ extensions as specified in the NIPRNet DMZ concept of operations (CONOPS).

xxiii) Ensure the DMZ extension provides web server, application server, and database server separations IAW SRGs and STIGS, as well as web application firewalling for all public facing applications.

xxiv) Require applications residing in DISA hosting environments to be implemented behind the DMZ extension architecture (as described in Communications Task Order [CTO] 10-065 [23 July 2010] and Task Order [TASKORD] 12-0371 [12 March 2012]) with actions in support of Increment 1 Phase 1 of the DOD NIPRNet DMZ Program.

xxv) Accept Certificates of Networthiness (CoNs) for applications under the following conditions:

(1) CoN will be IAW DOD memorandum, "Interim Guidance on Networthiness of Information Technology (IT) Connected to DOD Networks," 22 November 2011

(2) CoN will be signed by the partner AO or service-level CoN-issuing authority.

(3) CoN will be based on the networthiness assessment and can be leveraged or reused to support assessments by DISA.

(4) CoN will affirm the application has gone through a security review and compliance IAW the DOD Application Security and Development STIG.

(5) CoN applications will be hosted and monitored using DISA-provided capacity and DISA-supported OSs.

(6) CoN applications will not adversely affect the security posture of the underlying OE which includes all components below the application level.

(7) CoN applications will not require administrative privileges to the underlying OE.

(8) CoN application will not require configuration management (CM) control of the underlying OE.

(9) DISA will patch and maintain the security posture of the underlying OE without partner consent.

NOTE: If any of these CoN conditions cannot be met, DISA will require a copy of an existing authorization decision

xxvi) Destroy storage media IAW Procedures for the Offsite Use of the LM-1 Degaussers and DF-4 Hard Drive Destroyers tactics, techniques and procedures (TTPs).

xxvii) Maintain a system for managing access control to the OSs and its supported utility software.

xxviii) Authorize limited root access for the purpose of loading or configuring applications via the OOB network.

xxix) Authorize and enable full root access to production information systems only when applications are moved to T&D environments.

xxx) Revoke root access prior to information system promotion into a DISA production environment.

xxxi) Provide IA/security services as outlined in the DISA Service Catalog:

(1) Mainframe (IBM) http://disa.mil/Computing/Mainframe-Hosting/IBM.

(2) Mainframe (IBM Linux on System Z) http://disa.mil/Computing/Mainframe-Hosting/IBM-LINUX.

(3) Mainframe (UNISYS) http://disa.mil/Computing/Mainframe-Hosting/UNISYS.

(4) Server Hosting (Server Hosting and Virtualization) http://disa.mil/Computing/Server-Hosting/Server-Hosting-and-Virtualization.

c) Partners shall:

i) Update and maintain valid authorization decisions signed by the partner AO for partner information systems and applications in implementation or sustainment.

ii) Update the information system package to reflect the DISA environment within 90 business days of being declared FOC.

iii) Test, direct, and approve information systems and application security fixes and vendor-recommended software maintenance IAW DOD, USCYBERCOM, JFHQ-DODIN, Joint Staff, and DISA regulations, directives, guidelines and other proper authority. This includes, but is not limited to, IAVM notifications (IAVAs, IAVBs, and IAVTs), CVEs, SRGs, and STIGS.

iv) Be held responsible for spillages and accumulated restoration costs.

NOTE: The minimum amount charged to partners for DEE NDCIs is $2,500 per incident.

v) Provide cybersecurity documentation for new and amended workload implementations to include, but not limited to:

(1) Current and updated DIACAP or RMF authorization decisions.

(2) AO risk acceptance documentation (e.g., Residual Risk Statements).

(3) Proof of cybersecurity information systems and applications compliance.

(4) Proof of information systems PPSM registration.

(5) System security plans.

(6) Risk assessments.

(7) POAMs and mitigations.

vi) Implement and maintain cybersecurity functions related to information systems for which DISA is not providing database administration, web administration, and application support administration services.

vii) Maintain copies of DD Form 2875s for active users for system accounts being managed (e.g., additions, deletions, modifications, unlocking) and provide the forms to DISA upon request.

viii) Maintain access control for users to their applications;

ix) Provide written identification of all CUI, PII, HIPAA, and PCI applications and information being hosted by DISA.

x) Develop applications that interface and exchange identification and authentication with the security products used by DISA and the DOD, USCYBERCOM, JFHQ-DODIN, Joint Staff, and DISA regulations, directives, guidelines, and other proper authority.

xi) Use domain name service (DNS) names versus hard-coded IP addresses in application configurations (where possible) to avoid downtime when IP addresses change.

10.0 Audits and Audit Readiness for Systems Impacting Financial Statements

1) The Office of the Under Secretary of Defense (Comptroller) (OUSD[C]) Financial Improvement and Audit Readiness (FIAR) guidance specifies the need for an agreement that articulates the service receiver and service provider relationship and the applicable audit aspects for transactions relevant to the reporting entity financial statements.

2) This section describes the standard responsibilities of DISA and DISA's partners for supporting audit readiness efforts and audits affecting DOD financial statements and service providers.

3) Anything regarding audit readiness that falls outside of the standard support documented below must be negotiated with DISA and documented in Section 8.0 of the partner's SLA. Additional costs to accommodate associated non-standard requirements could potentially initiate an LE and the need for additional funding from the partner. Memorandums of agreement (MOAs), memorandums of understanding (MOUs), or other individualized agreements will not be developed or accepted as addendums, or in place of, the information documented in the SLA.

   NOTE: Auditing support is available for milCloud Plus. Partners using milCloud IaaS shall implement auditing in compliance with their Component policies.

4) DISA and partners shall:

   a) Maintain open communication and coordinate with each other and supporting contractors.

   b) Provide additional system information within agreed upon timeframes.

   c) Provide access to subject matter experts or contractors supporting those organizations within agreed upon timeframes.

   d) Discover and correct audit impediments that fall within the responsible party's/parties' organizational/authoritative jurisdiction(s).

   e) Establish a common, detailed understanding of the scope, roles, responsibilities, required FIAR deliverables, timeline, and method for obtaining assurance (e.g., through the completion of a DISA's Attestation Standard No. 801 (AT 801), formally referred to as Statement on Standards for Attestation Engagements No. 16 (SSAE 16), examination or directly as part of partner's audit readiness efforts for the applicable partner-managed system).

5) DISA will:

   a) Prepare, evaluate, and remediate DISA processes, systems, controls, and supporting documentation to support the audit readiness and financial statement audit sustainment efforts of partners and their customers.

b) Understand and be prepared to support the audit readiness timeline of partners and their customers. This is conditional on partners informing DISA of audit and audit readiness activities early in the process as annotated below.

c) Prepare for and undergo an annual AT 801 examination for which the scope includes control objectives and control activities relevant to partners' and their customers' internal control over financial reporting, and that culminate with DISA's issuance of a Service Organization Controls (SOC 1) report no later than August 15th of each year.

d) Provide partners a description of the control objectives and activities. These objectives and activities may affect aspects of the partners control environment and are relevant to financial reporting. Information about these controls can be found as an attachment to this document as well as in DISA's hosting services AT 801 SOC 1 report.

NOTE: To access the Financial Audit Baseline Controls, please click on the paperclip icon to the left and double click on the attachment. In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.

6) Partners shall:

a) Deliver the overall mission for their systems to all DOD military and civilian employees and administer the planning, programming, budgeting, and execution for the system-related programs; remain accountable for keeping the systems operationally effective and available for their own use and use by the DOD community.

b) Review AT 801, which provides assurances needed for auditors and system owners. Any concerns must be addressed with DISA Cyber Services.

c) Ensure auditors and system owners rely on the AT 801 to the greatest extent possible.

d) Partners with financial systems hosted by DISA: Evaluate and, as appropriate, implement controls that address the "Complementary User Entity Controls (CUECs)" as identified in the most recent copy of AT 801 report (henceforth referenced as a Service Organization Controls 1 or "SOC1" report) provided by DISA.

e) Notify DISA of systems hosted at DISA that are relevant to financial reporting.

f) Inform DISA of audit and audit readiness activities early in the process in order to properly plan.

g) Ensure special system requirements are documented and made part of the SLA; for example, include records retention requirements.

7) Audit Support Requests:

a) Audit support requests related to hosting services must be submitted to DISA at the following address: DISA Ft Meade SE Mailbox SE4 Integration Center (disa.meade.se.mbx.se4-integration-center@mail.mil).

b) Requests for evidential matter must be submitted on the DISA standard form (the standard form can be requested at the above email address). Requests will be initially evaluated and acknowledged within one (1) business day. DISA will make every effort to return evidential matter in the requested period of time. If DISA is unable to support a requested time for completion, DISA will inform the partner and provide an estimated completion date. Partners should understand clarity and completeness of requests impacts DISA's ability to respond quickly and accurately.

c) Documentation of disaster recovery plans will not be released due to the sensitivity of the information; however, upon request, plans may be reviewed remotely or on site in a live session.

d) Recurring periodic requests must be directed through the standard Mission Partner Engagement Office (MPEO) (http://disa.mil/Computing/Engagement-Executive) channels and documented as part of the SLA. Examples of this type of request are periodic lists of system users and periodic reports of system activity, such as logs.

11.0 Cyber Defense

The roles and responsibilities detailed below apply only to those partners that have elected DISA to serve as the Cybersecurity Defense Service Provider (CDSP) for their programs/applications. For partners' programs/applications that reside within a DECC but have not aligned in writing with DISA as their CDSP, notification of suspicious traffic observed by Columbus Network Assurance (COLS-NA) will be supplied to the applicable CDSP via Tipper and subsequent CDSP actions will be performed by the partner CDSP.

For partner programs/applications that have traditionally received any of the functions detailed below by DISA, but are not aligned in writing with DISA, please coordinate with CDSP Requests (DISA Letterkenny AD RE List CDSP Requests disa.letterkenny.re.list.cdsp-requests@mail.mil) to have that documented appropriately.

DISA employs a documented reporting structure designed to facilitate sharing and collaboration of information among all stakeholders involved with defense of the DODIN. This reporting structure is also leveraged to alert mission owners of cyber incidents and to disseminate information in order to mitigate or correct conditions associated with that event. The success of the CDSP program relies heavily on timely collation, correlation, information analysis, and warning dissemination. Additionally, automated analytical tools and alerts of attacks in progress are essential to the CDSP process. This reporting structure must also be linked to intelligence, law enforcement, policy makers, and the Regional or Theater-level information systems community (both government and commercial). Coalition Network Operations (NetOps) Centers (CNCs)/Theater NetOps Centers (TNCs) incident reporting procedures must consider the information needs of the intelligence and operations communities for planning, coordinating, and implementing response options.

The following information outlines the CDSP roles and responsibilities for both the provider (DISA) and mission partners that have aligned to DISA as their CDSP. The partner SLA must clearly indicate whether the partner has aligned to DISA as their CDSP.

NOTE: CDSP services not provided to the partner by DISA either due to the partner declining that service (documented in the SLA) or technological, staffing, or mission infeasibility, must be performed by the partner themselves or by their Component head.

1) Malware Notification Protection (MNP)

a) DISA will:

i) Provide access to anti-virus/anti-malware software and updated signatures for NIPRNet and SIPRNet. Through subscription to the Net Defense virus list server, and other anti-virus organizations, provide warnings and updated information on malicious (spyware, viruses, malware, adware, etc.) code threats.

ii) Maintain a 24x7 virus response capability and respond to all partner reports of virus activity or requests for support.

iii) Maintain a current POC list for DOD-approved vendor support.

iv) Implement formal procedures to report emerging viruses to United States Cyber Command (USCYBERCOM) within reporting time requirements.

v) COLS-NA will incorporate already established Host Based Security System (HBSS) feeds into the analyst toolset for monitoring purposes once the partner has established an HBSS presence.

vi) Ensure proper protection of data in transit, IAW DOD policy.

b) The partner shall:

i) Ensure all components implement anti-virus/anti-malware (e.g. HBSS) software and maintain updated signatures for all NIPRNet and SIPRNet systems.

ii) Communicate HBSS alerts to COLS-NA for incident handling action.

iii) Maintain responsibility for compliance with USCYBERCOM requirements

iv) Conduct weekly anti-virus scans of network-connected devices IAW the DOD STIGs; develop/implement a program to identify infected assets; and rebuild, quarantine, or remove the asset from the network upon detection.

v) Ensure all Cyber Defense (CyDef) personnel are aware of DISA's 24x7 capability to assist with malware mitigation and maintain an up-to-date listing (NIPRNet/SIPRNet email, phone, secure phone, etc.) for contacting DISA.

vi) Ensure personnel understand how to conduct timely reporting of the detection of unknown/emerging malware to DISA.

vii) Work with DISA to obtain Reverse Engineering/Malware Analysis (RE/MA) support if malware is identified (reference Incident Response – Analysis section for additional information).

2) Mission Partner Support and IA Training (S&T)

a) DISA will:

i) Assist the partner with identifying CyDef, NetOps, and IA security training requirements, upon request.

ii) Maintain configuration documentation received for partner networks to include: network diagrams, technical sensor/administrative, and policy POCs and related information.

iii) Alert the partner to vulnerabilities and provide timely technical solutions/assistance. Provide general and specific guidance on the hardening of the partner network components via STIG release.

iv) Work with Education, Training, and Awareness (ETA) providers to incorporate CyDef requirements into ETA curricula and courseware and provide course development technical support in the areas of network protections, malicious code, Information Operations Condition (INFOCON)/Cyber Operations Condition (CYBERCON) and IAVM.

v) Notify the partner of any CM changes or changes/activities that could affect NetOps.

vi) Share sanitized partner data and items of interest with the network assurance community.

b) The partner shall:

i) Maintain, and provide to DISA upon request, accurate CM documentation as required. Documentation that has been reviewed within the last year to include (but not limited to): network diagrams, software and hardware inventories and network ports, protocols and services (PPS) listing, technical sensor/administrative and policy POCs lists and related information.

ii) Provide situational awareness to DISA of any known vulnerabilities, mitigation strategies, major changes to the network, or other actions that would affect DISA's ability to protect partner networks.

iii) Maintain DISA guidelines for the hardening of networks (e.g. STIGs) and inform DISA of any significant changes to the security or architecture of the networks (e.g. architecture redesign, addition/removal of critical servers or infrastructure).

(1) Refer to the IA Support Environment (IASE) for network hardening guidelines: http://iase.disa.mil.

(2) Inform DISA of any changes by sending an email to DISA.letterkenny.RE.list.cdsp-requests@mail.mil.

iv) Identify and provide asset data on critical network assets (servers, security devices, network devices, DNS, Primary Domain Controllers [PDCs], Backup Domain Controllers [BDCs], etc.) so DISA can more accurately assess risk to those assets.

v) Notify DISA of any CM changes involving connectivity, to include location, sensor name, Command Communication Service Designators (CCSDs), bandwidth, IP address space, and/or backend connections or changes that could affect NetOps.

Inform DISA of any changes by sending an email to DISA.letterkenny.RE.list.cdsp-requests@mail.mil.

This information must be provided to
NIPR: DISA.letterkenny.RE.mbx.CDSPsubmission@mail.mil
SIPR: DISA.letterkenny.RE.mbx.CDSPsubmission@mail.smil.mil

3) INFOCON Compliance/NetOps Awareness

a) DISA will:

i) Maintain the latest DOD guidance and procedures for the INFOCON/ CYBERCON reporting process, formats, directive actions, and security.

ii) Provide notification to the partner of all changes to the global and theater (where appropriate) INFOCON/CYBERCON level, and recommend actions in response to any changes to the INFOCON/CYBERCON level or Targeted Response Options (TROs). Monitor partner INFOCON/CYBERCON status, and advise USCYBERCOM of any changes.

iii) Provide guidance at least annually to the partner on directed measures to protect their networks in response to INFOCON/CYBERCON levels 5 through 1.

b) The partner shall:

i) Ensure all partner organizational elements implement appropriate INFOCON/CYBERCON levels. Immediately notify DISA of any partner-directed change in INFOCON/CYBERCON level or TROs.

ii) Maintain the latest DOD guidance and procedures for the INFOCON/ CYBERCON reporting process, formats, directive actions and security.

iii) Provide a read-only view in DOD approved vulnerability repository of assets and POC information to DISA for situational awareness of vulnerability status and mitigation strategies.

4) Information Assurance Vulnerability Management (IAVM)

a) DISA will:

i) Analyze feedback received on the relationship between IAVM status of partner assets and any malicious incidents that occur.

ii) Provide feedback and recommendations to the partner.

b) The partner shall:

i) Maintain compliance with IAVM program directives and vulnerability response measures.

ii) Ensure the proper acknowledgement and reporting of IAVM notices via generated messages. Appropriate personnel (e.g. IA Manager [IAM], Information System Security Manager [ISSM], system administrator [SA]) must have and maintain active accounts in a DOD approved vulnerability repository.

iii) Establish a comprehensive Vulnerability Management Plan, including vulnerability remediation, STIG compliance management, and patch testing.

iv) Provide feedback to DISA on the relationship between the IAVM status of assets and any malicious incidents that occur.

5) Network Security Monitoring (NSM)/Intrusion Detection

a) DISA will:

i) Use formal network security monitoring policies and procedures that include the appropriate use of DOD-approved Intrusion Detection and Prevention System (IDPS) tools that have automated alert capabilities enabled.

ii) Perform detection (monitoring and analysis) activities on the CCSDs or IP space/range if CCSDs aren't applicable, using intrusion detection sensors/intrusion prevention sensors (Intrusion Detection System [IDS]/ Intrusion Prevention System [IPS], hereafter called sensors. Activity will occur on a 24x7 basis via the DISA NetOps Centers (DNCs)/COLS-NA.

iii) Follow documented procedures for characterizing anomalous events detected by sensors and other network monitoring systems.

iv) Monitor the partner's unclassified and classified networks. Provide CDSP failover continuity of operations (COOP) in the event of an outage at the service provider location.

v) Review and analyze logs in a timely manner to detect intruders, and within 30 minutes of detection of an event, begin preliminary analysis of the event. Follow documented procedures to obtain copies of partner audit/system logs.

vi) COLS-NA will incorporate already established HBSS feeds into the CDSP analyst toolset.

b) The partner shall:

i) Develop a local AO-approved program to use approved network security monitoring tools.

ii) Ensure all components implement anti-virus/anti-malware (e.g. HBSS) software and maintain updated signatures for all NIPRNet and SIPRNet systems.

iii) Develop and maintain documented policies and procedures for assessing baseline configuration guidelines, and maintaining the continued update of security standards.

iv) Provide audit/log files to DISA as requested for correlation activities.

v) Aid DISA in determining the optimum location of sensors. Provide DISA with unclassified and classified network topology diagrams representing all enclaves being monitored. The partner/DISA shall mutually agree on sensor placement.

vi) Ensure sensors purchased are the size/model recommended by DISA.

6) Attack Sensing and Warning (AS&W)

a) DISA will:

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

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

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

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

v) Provide Intrusion Assessment support for identified suspicious/malicious activities that are indicative of a compromise without a confirmed compromise.

vi) Share sanitized partner data collected with the NA community via secure channels.

b) The partner shall:

i) Ensure AS&W information is appropriately disseminated within the partner and its sub-components.

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

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

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

7) Indications and Warning (I&W)

a) DISA will:

i) Develop TTPs to provide the partner with intelligence-based potential computing threats and expected imminent actions on a timely basis. These warnings will be based on intelligence community and other sources. Situational awareness will also be provided to the partner based on theater activities and those threats and activities correlated from other entities (e.g., USCYBERCOM and DNCs/COLS-NA).

ii) Follow a documented methodology for sharing information with the intelligence community via proper channels, and for checking non-governmental and counterpart CDSP organizational websites for threat and warning notifications daily to ensure situational awareness.

iii) Coordinate within DISA and with the partner to consolidate and correlate situational awareness data into a single integrated picture.

b) The partner shall:

i) Acknowledge, maintain, and reference any threat reports disseminated by DISA or other sources.

ii) Ensure I&W and situational awareness information is appropriately disseminated within the organization, and daily command situational awareness is shared with DISA.

8) Incident Reporting

a) DISA will:

i) Report potential incidents and correlated information from these incidents/events that occur on DISA-monitored sensors using documented procedures IAW DOD guidance. These events/incidents will be provided to partners and reported to USCYBERCOM.

ii) Ensure incidents are populated into the DOD enterprise incident database. DISA is the conduit to USCYBERCOM for all CyDef incidents.

iii) Follow documented policies and procedures for handling incidents reported to law enforcement and counterintelligence agencies.

iv) Retain all incident reports (electronic or paper) for at least one year.

v) Share sanitized partner data collected with the NA community via secure channels.

b) The partner shall:

i) Develop and implement a process with formal documented procedures to conduct incident handling IAW DOD/Chairman of the Joint Chiefs of Staff (CJCS) incident handling procedures.

ii) Self-report all incidents and questionable events for covered networks in a timely manner to DISA as discovered. DISA will enter incidents into the DOD enterprise incident database on behalf of the partner. To report an incident please contact disa.columbus.eis.mbx.cols-esdna@mail.mil.

Follow documented procedures as instructed in the DISA First Responders Guide (FRG).

iii) Verify or validate incidents identified by DISA, along with any operational impact, and provide feedback to DISA in a timely manner.

iv) Retain soft or hard copies of all applicable incident reports for one year.

v) Follow documented procedures as instructed in the FRG in coordination with COLS-NA.

9) Incident Response – Analysis (IRA)

a) DISA will:

i) Provide analysis of incidents IAW documented policies and procedures that incorporate methods to determine the threat, risk, or damage an incident may impose on partner networks. The analysis will be based on either or both of the following:

(1) Any similar events or activities in theater and/or across the DOD networks.

(2) Current attack or malicious code information. DISA will collaborate with USCYBERCOM Joint Chiefs Operations (J3) and Joint Chiefs Intelligence (J2) analysts and CDSP peer organizations as appropriate.

ii) Provide Volatile Data Analysis (VDA) and Forensic Media Analysis (FMA) as requested or required.

iii) Provide RE/MA for suspicious files as requested or required.

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

v) Operate on a 24x7 basis. A recall roster is not required, 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 days.

vi) Share sanitized customer data collected with the COLS-NA community via secure channels.

b) The partner shall:

i) Self-report all incidents and questionable events for covered networks in a timely manner to DISA as discovered. DISA will enter incidents into the DOD enterprise incident database on behalf of the partner.

ii) Follow documented procedures as instructed in the DISA FRG

iii) 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.

iv) 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.

v) Provide local technical hands-on assistance as required to any team deployed for on-site support.

vi) Share sanitized collected data with the COLS-NA community via secure channels.

10) Incident Handling Response (IHR)

a) DISA will:

i) Develop and exercise documented incident handling and response procedures that specify when and how to escalate a response. Inform analysts about the procedures and how to apply them. Using these procedures, maintain a 24x7 incident/event handling capability and recommend actions the partner should take in response to an on-going or post-discovery incident. This may include port or protocol blocks or other actions.

ii) Provide rapid response and recovery actions for widespread or seemingly uncontainable intrusion activity as directed by the DISA Command Center (DCC) or as requested by the partner.

iii) Use a robust, automated tool (Remedy) to track incident response ticketing.

iv) Review and distribute updated incident response guidelines, checklists, and recommended procedures at least annually.

v) Maintain an incident/event handling operations Master Station Log. Entries will be kept up-to-date and complete.

vi) Share sanitized partner data collected with the COLS-NA community via secure channels.

b) The partner shall:

i) Develop a program to allow for proper incident handling and response. Provide follow up and feedback to DISA on the recommended actions.

ii) Track incidents, support the response process, and generate managerial reports.

iii) Obtain and maintain an active, classified means (e.g. SIPR account, Secure Telephone Equipment [STE]) for sufficient technical and managerial personnel to cover the potential for 24x7 incident response. 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.

iv) Share sanitized collected data with the COLS-NA community via secure channels.

v) Provide funding for additional Incident Response as required if an Intrusion Assessment or Incident Response has already been completed in the FY.

vi) If the partner is unavailable during off-hours, the CDSP reserves the right to escalate the incident. If no partner is available, the CDSP has the authority to turn off connection until either of the following occur:

(1) The incident is resolved
(2) The partner comes in contact with CDSP and a mutual closure/resolution is made.

DISA also offers the services below, though mission partners are not automatically receiving or entitled to those services via their use of the DECC infrastructure. The partner's SLA must reflect whether any of the additional services below are applicable.

1) Vulnerability Analysis and Assessment (VAA) Support

2) VAA – External Vulnerability Scans (EVS)

3) VAA – Web Vulnerability Scanning (WVS)

4) VAA – Other Services

12.0 Dispute Resolution

An alternative Dispute Resolution clause is as follows:

1) Dispute resolution involves the program offices, resource management office, accounting offices, KO, and agency's Chief Financial Officer (CFO), as appropriate. Disputes must be documented in writing with clear reasons for the dispute. An MOA must 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 may not chargeback or reject transactions that comply with these rules. Further, new transactions may not be created to circumvent these rules. Transactions that comply with these rules, but are disputed, will 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 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 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 may 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 an SLA has been breached by either party, DISA will identify the circumstances behind the incident. The resolution could take many forms (e.g., a Service Improvement Plan [SIP] that is referred to the DISA Problem Management team or a modification to an SLA).

13.0 Additional Responsibilities

1) DISA will 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 will 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 DISA if requested.

4) DISA will 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

5) DISA and the partner shall furnish all notifications and information to one another in writing via memorandum or electronic mail and by telephone, if urgent.

6) DISA will meet with partner representative(s) to discuss performance; issues; areas of concern; anticipated workload changes; and any changes or modifications to the Agreement, Business Continuity Plan (BCP), or Risk Assessment and/or security posture.

7) The partner shall work with the appropriate DISA representative to provide any required input into the development of the partner's application recovery procedures.

8) To successfully integrate an application into the Continuity of Operations /Service Continuity program, there are certain responsibilities which cannot be performed by DISA. The partner shall:

   a) Maintain a valid authorization decision signed by the partner AO.

   b) Initiate requests for COOP capability exercises through the assigned 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) Initiate termination or removal of COOP coverage for server-based processing.

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

9) The partner shall provide full, detailed documentation for any change requests recommended by DISA to improve the performance or security position of the partner workload with which the partner non-concurs, providing specific information regarding the

problem(s) the change request would introduce and/or specific reasons why the change request cannot be implemented at the time with which it is non-concurred.

10) When available, DISA Enterprise services (e.g., DEE, DEPS) must be used in lieu of partner-unique application solutions.

11) DISA will furnish to the partner a primary and alternate DISA POC, documented in the SLA, and update these as necessary.

12) DISA will furnish to the DISA service desk both the primary and alternate partner POCs and update them when necessary. In the event the service desk cannot contact the primary POC, the alternate on the list will be contacted. The partner POC shall notify the partner users of any operational situations that impact service.

13) The partner shall coordinate with DISA on any exceptions to normal processing as soon as they become known. DISA will 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.

14) For a defense business system modernization, the partner shall 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 for submitting a copy of the DBSMC certification results or certification control number for the proposed business system to DISA prior to DISA obligating funding for services. Failure to present the appropriate documentation precludes DISA from taking further action or providing services until the time documentation is submitted.

    Defense business system modernization: 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).

    Reference USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2222 Defense business systems: architecture, accountability, and modernization.

    Documentation for above must be provided as part of the partner's acceptance of any BMMP solution offered by DISA before implementation of the project can proceed.

    Office of the Deputy Chief Management Officer Defense Business Council (DBC) and Investment Review Board (IRB):
    http://dcmo.defense.gov/Governance/DefenseBusinessCouncil.aspx.

14.0 Performance Standards

These performance standards are available to all DISA partners.

DISA will make a good faith effort to meet or exceed the following operational objectives. Circumstances beyond DISA control (e.g., commercial power outages, natural disasters, inefficient application software releases, partners' local communications problems) are excluded. DISA 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 DISA 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 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	As requested	Provides previous month's capacity utilization reports for 1) most DISA-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 MIPRs at the service level.

15.0 Global Content Delivery Service Performance Standards and Responsibilities

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

DISA:

1. Will provide immediate failover to a redundant GCDS node for disaster recovery.
2. Will provide GSD (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. Is not responsible for the content, look, and feel of the website and/or the partner apology page.
8. Is not responsible for broken links on a website or failure of pages or graphics to load on the page.
9. Will monitor the integrated URLs accessibility, performance, and status 24x7/365 on both the NIPRNet and SIPRNet.
10. Will notify the partner immediately if there is a technical issue related to their application.
11. Will notify NetStorage subscribers if their NetStorage allocation is reaching capacity.
12. Will decommission an integrated URL 30 days following a partner’s decommission action. Will not refund integration costs if the URL has gone live on GCDS.
13. Will provide streaming service over the NIPRNet or SIPRNet only to the partners.
14. Will assist the partner with the setup and configuration of the encoder for the streaming event.
15. Will assist the partner with a test and rehearsal prior to the event.
16. Will schedule support for the partner’s streaming efforts via the respective DISA Mission Partner Engagement Executive team.
17. Will provide the partner with documentation to set up the streaming service.
18. Will provide the configured video stream to a global audience on the NIPRNet or SIPRNet.
19. Will provide the partner a unique URL for dissemination to the target audience.
20. Upon request, can enable digital video recorder (DVR) capabilities for the live broadcast for 48 hours to support different time zones (Should the partner wish to retain the broadcast for longer than 48 hours, integration into GCDS NetStorage will be required).

21. Is not responsible for the hardware or software based media encoders used for the streaming event.
22. Is not responsible for the performance of the software-based media encoder on the computer (as a general rule, the more powerful, the better).
23. Is not responsible for troubleshooting of the network or firewall configurations at the partner's site.
24. 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.

GCDS:

1. 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 will ensure an apology page created by the partner is displayed until the origin server is re-connected or is operational again.
2. Will ensure the partner's performance metric interface, the GCDS Portal, is available to the partner 95% of the time.
3. Will provide updates to the GCDS partners via the GCDS website at http://www.disa.mil/Services/Enterprise-Services/Infrastructure/GCDS.
4. Will not decommission a URL without the partner's written consent.
5. Will not troubleshoot an application if the triage does not indicate it is a GCDS problem.
6. Will not continue integration if all 40 hours per URL are used up during the integration process.
7. Will not re-integrate a URL if the partner has decommissioned the URL from GCDS and the URL was decommissioned from GCDS.

DISA Partner:

1. Shall notify the appropriate DISA Mission Partner Engagement Executive team in writing of their intent to decommission two weeks prior to decommission.

8. Shall enable log storage on GCDS through the GCDS portal (part of the integration process).
9. 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.
10. Has the flexibility to purge an event or the entire content. If the file is purged by accident, the partner shall notify GCDS via the GSD (Email: disa.columbus.esd.mbx.gcds-columbus@mail.mil) to attempt to recover the file.
11. Understands the data is unavailable to the end users until the propagation from the origin server is completed across the GCDS network if their entire content is purged intentionally or accidentally. Shall provide written consent to GCDS should they wish to decommission a URL.

12. Has the flexibility to decommission a URL. If this occurs, the partner understands 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.
13. Shall inform the GCDS PMO anytime a POC responsible for the management of the integrated application changes.
14. Is responsible for maintaining the allocation if the partner uses GCDS NetStorage.
15. Is responsible for ensuring the IA accreditation of the application is maintained. If the accreditation expires, the partner shall notify the GCDS PMO immediately to suspend content delivery until the application is re-accredited.
16. 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.
17. Understands if they were brought onto GCDS with an LE, the recurring billing for GCDS stopped on September 30, 2011 due to the GCDS transition to the DISN Subscription Service (DSS).
18. Is responsible for the procurement of the broadcast media (camera, hardware or software-based encoder, production equipment).
19. Is responsible for the opening of the required ports on the local firewall to enable the streaming.
20. If using a hardware-based encoder, is responsible for the proper IA authorization and accreditation for using the hardware-based encoder.
21. Is responsible for ensuring the selected media encoder is H.264 Industry Standard compliant.
22. Is responsible for the content and the operational security associated with the streaming event.
23. Shall contact the respective DISA Engagement Executive team to initiate the request for streaming support.
24. If subscribing to NetStorage, may request an 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.

Appendix A – Acronyms

The following acronyms are referenced throughout this T&C.

Acronym	Definition
AO	Authorizing Official
ASC	Application System Code
ASI	Automated System Interruption
AS&W	Attack Sensing and Warning
AT	Attestation Standard
ATC	Authorization to Connect
ATD	Authorization Termination Date
ATO	Authorization to Operate
ATOC	Authorization to Operate with Conditions
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
CAL	Category Assurance List
CAP	Connection Approval Process
CAR	Customer Account Representative
CCC	Central Communications Center
CCSD	Command Communication Service Designator
CDC	Core Data Center
CDSP	Cybersecurity Defense Service Provider
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, Availability
CIC	Customer Identification Code
CIS	Centralized Invoice System
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CL	Confidentiality Level

Acronym	Definition
CM	Configuration Management
CNC	Coalition NetOps Center
CND	Computer Network Defense
COI	Community of Interest
COLL	Collection
COLS-NA	Columbus Network Assurance
CoN	Certificate of Networthiness
CONOPS	Concept of Operations
COOP	Continuity of Operations
CORA	Certificate of Risk Assessment
COTR	Contracting Officer's Technical Representative
COTS	Commercial off-the-Shelf
CPU	Central Processing Unit
CTO	Communications Task Order
CUEC	Complementary User Entity Control
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CYBERCON	Cyber Operations Condition
CyDef	Cyber Defense
DAA	Designated Approving Authority
DADMS	Department of the Navy Applications and Database Management System
DATO	Denial of Authorization to Operate
DBC	Defense Business Council
DBSMC	Defense Business Systems Management Committee
DCAS	Defense Cash Accountability System
DCC	DISA Command Center
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DIP	DISA Inherited Policy
DISB	Disbursement
DISR	DOD Information Technology Standards Registry
DITPR	DOD IT Portfolio Repository
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
DNC	DISA NetOps Center
DNS	Domain Name Service
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DON	Department of the Navy
DPAS	Defense Property Accountability System
DVR	Digital Video Recorder
E2E	End-to-End
EBN	Enterprise Backup Network
ECA	Enclave Connection Authority
ECA	External Certificate Authority
EIBN	Enterprise Infrastructure Backbone Network
ELO	External Liaison Officer
eMASS	Enterprise Mission Assurance Support Service
EOC	Enterprise Operations Center
EOL	End-of-Life
ETA	Education, Training, and Awareness
EULA	End User License Agreement
EVS	External Vulnerability Scan
FC	Fibre Channel
FIAR	Financial Improvement and Audit Readiness
FISMA	Federal Information Security Management Act
FMA	Forensic Media Analysis
FMLO	Financial Management Liaison Office
FMR	Financial Management Regulation
FOC	Full Operational Capability
FRG	First Responders Guide
FY	Fiscal Year

Acronym	Definition
GAO	General Accounting Office
GOTS	Government off-the-Shelf
HBA	Host Bus Adapter
HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
IA	Information Assurance
IaaS	Infrastructure as a Service
IAC	Invoice Account Code
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IATT	Interim Authorization to Test
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAVTA	Information Assurance Vulnerability Technical Advisory
IAW	In Accordance With
IBE	Initial Business Estimate
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IECA	Interim Enclave Connection Authority
IFAS	Industrial Fund Accounting System
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
IPSec	Internet Protocol Security
IPAC	Intra-Governmental Payment and Collection System
IRA	Incident Response – Analysis
IRB	Investment Review Board
ISSM	Information System Security Manager

Acronym	Definition
ISSO	Information System Security Officer
IT	Information Technology
I&W	Indications and Warning
J2	Joint Chiefs Intelligence
J3	Joint Chiefs Operations
JFHQ-DODIN	Joint Force Headquarters – Department of Defense Information Network
JTA	Joint Technical Architectural
KO	Contracting Officer
LE	Letter Estimate
LECA	Local External Certification Authority
LIECA	Local Interim External Certification Authority
MAC	Mission Assurance Category
MNP	Malware Notification Protection
MIAG	Mandatory IA Guidance
MIPR	Military Interdepartmental Purchase Request
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPEO	Mission Partner Engagement Office
NAS	Network Attached Storage
NDCI	Negligent Discharge of Classified Information
NetOps	Network Operations
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSM	Network Security Monitoring
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 (Comptroller)
PCI	Payment Card Industry
PDC	Primary Domain Controller
PE	Planning Estimate

Acronym	Definition
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Period of Performance
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
PR/SM	Processor Resource/System Manager
RE/MA	Reverse Engineering/Malware Analysis
RMF	Risk Management Framework
RRP	Resource Request Process
RTO	Red Team Operation
SA	System Administrator
SAN	Storage Area Network
SDLC	System Development Life Cycle
SDP	Service Delivery Point
SEA	Server Enterprise Architecture
SIP	Service Improvement Plan
SIPRNet	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SO	System Owner
SOC	Service Organization Controls
SSAE	Statement on Standards for Attestation Engagements
SSL	Secure Socket Layer
SRF	Service Request Form
SRG	Security Requirements Guide
StEA	Storage Enterprise Architecture
STIG	Security Technical Implementation Guide
STE	Secure Telephone Equipment
T&C	Terms and Conditions
T&D	Test and Development
TAS	Treasury Account Symbol

Acronym	Definition
TASKORD	Task Order
TNC	Theater NetOps Center
TRO	Targeted Response Option
TTPs	Tactics, Techniques and Procedures
USAF	United States Air Force
USC	United States Code
USCC	United States Cyber Command
USCYBERCOM	United States Cyber Command
VAA	Vulnerability Analysis and Assessment
VDC	Virtual Data Center
VDA	Volatile Data Analysis
VLAN	Virtual Local Area Network
VOE	Virtual Operating Environment
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WCF	Working Capital Funds
WVS	Web Vulnerability Scan
z/Linux	Linux on System z

Appendix B – Glossary

Term	Description
Accreditation (DIACAP)	Formal declaration by a DAA that an information system 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 [Legacy])
Authorization to Operate (ATO)	Authorization granted by a DAA/AO for a DoD information system to process, store, or transmit information. An ATO indicates a DoD information system has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA/AO. ATOs may be issued for up to 3 years. (DODI 8510.01)
Authorization (RMF)	Formal declaration by an AO that an information system 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)
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)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
Certification	Comprehensive evaluation of the technical and non-technical security features of an information system 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 [Legacy])
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 DISA who serves as the primary POC to the partner for DISA services. The CAR is responsible for ensuring the partner is satisfied with DISA services.
Designated Approving Authority (DAA) / Authorizing Official (AO)	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.
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 information systems. The DOD Public Key Infrastructure (PKI) 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 DISA 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.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Initial Operational Capability (IOC)	A system reaches IOC when the application has been loaded, tested, and opened to the user base for production.
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.
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.

Term	Description
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 DISA 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 Authorization to Connect (ATC) is differentiated from ATC as is described in DISA Connection Approval Process (CAP) documents, and in this document only applies to DISA internal processes. The MIAG contains the complete list of documentation required to be submitted to the approving authority for approval.
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 DISA internal processes. For this process, the required documentation is an email containing the following information: • device name • IP address of the new device • hosting site • managing site • connection type requested ISSM 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 must have sufficient lead-time to permit appropriate resource adjustments to be made. Negotiations will be between the DISA and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA will remain in effect. *NOTE: For small modifications such as POC updates, formal approval is not necessary but all parties must be informed of the change.*
Negligent Discharge of Classified Information (NDCI)	An NDCI occurs when classified information is introduced to a system above the level of classification for which the system is authorized or accredited.

Term	Description
Operating Environment (OE)	The OS on the server, i.e., Windows, Linux, or UNIX
Partner	The service or agency for which DISA provides services.
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Plan of Action and Milestones (POA&M)	A document identifying tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Planning Estimate (PE)	An estimated project cost for sustainment of services provided to the partner each FY (Oct – Sept).
Privileged User	A user authorized (and, therefore, trusted) to perform security-relevant functions ordinary users are not authorized to perform.
Renewal	The partner and DISA 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 must be renewed no less than annually and must be reconciled to the SLA as part of an annual SLA review. Negotiations will be between the DISA and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA will remain in effect indefinitely.
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Term	Description
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.
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 DISA provides to the 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 DISA and the partner.

Appendix C – References

Both parties shall comply with directives, instructions, regulations, and guidance issued by DISA, DOD, and OMB including, but not limited to:

1) CJCS Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011 (Directive Current as of 9 June 2015)
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

2) DISA Instruction 210-225-2, Privacy Program, 10 June 2013
http://www.disa.mil/About/DISA-Issuances/~/media/Files/DISA/About/Publication/Instruction/di2102252.pdf

3) DISA Instruction 630-225-8, Information Services Freedom of Information Act (FOIA) Program for DISA, 5 February 2014
http://www.disa.mil/About/DISA-Issuances/~/media/Files/DISA/About/Publication/Instruction/di6302258.pdf

4) DISA Memorandum, Subject: DISA Vulnerability Management Policy, 25 April 2016

5) DOD Directive (DODD) 5105.19, Defense Information Systems Agency (DISA), 25 July 2006
http://www.dtic.mil/whs/directives/corres/pdf/510519p.pdf

6) DODD 8500.01E, Information Assurance (IA), 24 October 2002 (Certified Current as of 23 April 2007)
http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf

7) DOD FMR 7000.14-R, June 2011
http://comptroller.defense.gov/fmr

8) DOD FMR 7000.14-R, Volume 11B, Reimbursable Operations Policy – Working Capital Funds (WCF), April 2013
http://comptroller.defense.gov/Portals/45/documents/fmr/Volume_11b.pdf

9) DODI 4000.19, Support Agreements, 25 April 2013
http://www.dtic.mil/whs/directives/corres/pdf/400019p.pdf

10) DODI 5200.01, DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI), 21 April 2016
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

11) DODI 8500.01, Cybersecurity, 14 March 2014
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

12) DODI 8500.2, Information Assurance (IA) Implementation, 6 February 2003
http://www.cac.mil/docs/DoDD-8500.2.pdf

13) DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), 12 March 2014 (Incorporating Change 1, Effective 24 May 2016) *(formerly DOD Information Assurance Certification and Accreditation Process [DIACAP], November 2007)*
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

14) DODI 8551.01, Ports, Protocols, and Services Management (PPSM), 28 May 2014 http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

15) DODI 8530.01, Cybersecurity Activities Support to DOD Information Network Operations, 7 March 2016 *(Incorporates and cancels DODI O-8530.2)* http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf

16) DOD Internet-NIPRNet DMZ Technology Security Technical Implementation Guide (STIG) Overview, Version 3, Release 1, 6 July 2015 https://disa.deps.mil/ext/cop/iase/stigs/Documents/fouo_dod_internet-niprnet_dmz_technology_v3r1_stig.zip

17) DOD Joint Technical Architecture Volume II, Version 6.0, 3 October 2003 www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA443892

18) DOD Manual 5200.01, Volume 3, DOD Information Security Program: Protection of Classified Information, 24 February 2012 (Incorporating Change 2, 19 March 2013) http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

19) DOD Memorandum, Interim Guidance on Networthiness of Information Technology (IT) Connected to DOD Networks, 22 November 2011 http://www.disa.mil/network-services/~/media/Files/DISA/Services/UCCO/DoD_Networthiness_Memorandum.pdf

20) Federal Information Security Management Act of 2002 http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

21) GAO-03-584G, United States General Accounting Office (GAO) Executive Guide, Information Technology, A Framework for Assessing and Improving Enterprise Architecture Management, Version 1.1, April 2003 http://www.gao.gov/new.items/d03584g.pdf

22) National Defense Authorization Act for Fiscal Year 2014, December 2013 http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT86280/pdf/CPRT-113HPRT86280.pdf

23) NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (Includes Updates as of 22 January 2015) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

24) Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, 8 February 1996 http://www.whitehouse.gov/omb/circulars_a130

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

26) Security Technical Implementation Guides (STIGs) http://iase.disa.mil/stigs/Pages/index.aspx

27) United States Code (USC), Title 10, Subtitle A, Part I, Chapter 7, Section 186, Defense Business System Management Committee, 3 January 2007

http://www.gpo.gov/fdsys/granule/USCODE-2006-title10/USCODE-2006-title10-subtitleA-partI-chap7-sec186/content-detail.html

28) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2208, Working-Capital Funds, 3 January 2012 http://www.gpo.gov/fdsys/granule/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partIV-chap131-sec2208/content-detail.html

29) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2222, Defense Business Systems: Architecture, Accountability, and Modernization, 3 January 2012 https://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/pdf/USCODE-2011-title10-subtitleA-partIV-chap131-sec2222.pdf

30) USCC TASKORD 13-0613, Directive to Scan Public DOD Websites for Vulnerabilities, June 2013 https://www.cybercom.smil.mil (*NOTE: This is a SIPRNet link; orders on bottom right)*

Document Source

1) All DISA Instructions http://www.disa.mil/About/DISA-Issuances/Instructions

2) All DOD Issuances http://www.dtic.mil/whs/directives/

3) All OMB Circulars https://www.whitehouse.gov/omb/circulars_default