Defense Information Systems Agency
A Combat Support Agency

Defense Information Systems Agency

Terms and Conditions

Applicable to all Service Level Agreements

Published Date:
Nov 2018

Version FY19.0

Revision History

Date	Version Number	Section Reference	Changed By	Description
N/A	Old	All	BDM	Archived track changes can be obtained by contacting the BDM-MPEO team.
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

Date	Version Number	Section Reference	Changed By	Description
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
11/2016	6.2	Sect 3; former Sect 11; Sect 12,14	BDM52	Modified verbiage re: LE timeline for clarity (Sect3, Onboarding Paths); removed Cyber Defense section (former Sect11) (updates were made and new info is linked to in the DISA Service Catalog under CDSP: http://disa.mil/Cybersecurity/Network-Defense/CDSP); changed 10 calendar days to 10 business days in (Sect12, Additional Responsibilities, #13); updated GCDS fee and billing verbiage (Sect14) 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
5/2017	6.3	Sect 2,3,7-11; Appendices A,C	BDM42	Changed references of DECC to Computing Ecosystem Datacenters or Datacenters (throughout); made updates and clarified verbiage (Sect7-10,13); corrected format (Sect11); Updated IA references (AppC) Note: If you wish to view all changes in detail, please send a request for the track changed copy of this document to disa.meade.bd.mbx.disa-service-catalog-management@mail.mil.
6/1/2017	6.3.1	Sect 9; RMF Baseline Common Controls Spreadsheet	BDM42	Removed policy as an example of RMF common control providers in Sect 9 para 7.b.iii (p24); removed DISA Inherited Policies (DIP) tab from RMF spreadsheet until further reviews are completed.
9/2017	7.0	Throughout	SEL7	Updated the Cybersecurity section; added newly updated RMF attachments.
4/1/2018	8.0	Throughout	SEL, RMF	Updates to sections 9 and 10 (RMF). Added new RMF attachments. SEL (sections 7 and 8)

Date	Version Number	Section Reference	Changed By	Description
4/1/2018	8.0	throughout	OCF	Change E2E to DRMP. (2.0) Remove: or immediately upon passage of a Continuing Resolution or DOD Appropriations Act. (4.0) Change to: Non-Severable and Severable (implemenation and sustainment) (4.0) Remove entirely or update to reflect our current PE/Budget build process. (4.0 3a) Move to Section 1.0 Introduction 1) SLA (4.0 3b) Section 5.0 changes: -Revise language to state funding is required during the passage of a Continuing Resolution or DOD Appropriations Act -Remove paragraph. Already stated in previous sections. -Update with new MIPR instructions and Non-Severable/Severable language -Add language and instructions for multiple DoDAACs. -Update to: https://bert.csd.disa.mil -Replace with Severable and Non-Severable -Add Basic Services to: 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? (not sure if the cost has been included in the budget) Add business rule: DISA uses the OUSD FIAR list as the authoritative billing source. Partner application(s) must be identified as hosted at DISA on the list before DISA will start billing. (10.0)
11/15/2018	FY19.0	9.0-Cybersecurity	RMF Team	Update Section 9.0 to reflect changes to service pakcages.
11/15/2018	FY19.0	1.0	BDM4	Add verbiage regarding “one-time service”. Per direction from Mr. Jason Martin (SES)
11/15/2018	FY19.0	1.0	OCF – C. Stevens	Add verbiage regarding MP signatures on SLA within 30 business days.
11/15/2018	FY19.0	3.0	EWT – L. Bietsch	Changed A-Goal and C-Goal in body of T&C to Rate-Based and Reimbursable; DISA has gotten away from using the A-Goal and C-Goal terminology. Also changed the number of days from 10 to 5 that the EW team has to finalize IBEs and LEs once we accept the Estimate for Completion.

Table of Contents

1.0 Introduction 1
2.0 Onboarding Paths 3
3.0 Business Estimate Process 4
4.0 Pricing 8
5.0 Funding and Billing 9
6.0 Duration and Termination of Agreement 12
7.0 System Technology 14
8.0 Ownership and Licenses 17
9.0 Cybersecurity 21
10.0 Audits and Audit Readiness for Systems Impacting Financial Statements 30
11.0 Dispute Resolution 32
12.0 Additional Responsibilities 33
13.0 Performance Standards 35
14.0 Global Content Delivery Service Performance Standards and Responsibilities 36
Appendix A – Acronyms 1
Appendix B – Glossary 1
Appendix C – References 1

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.

    a. 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.

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

    Mission Partners must sign the SLA within 30 business days after receipt of the SLA with DISA signatures.

    NOTE: The SLA only contains services provided on a recurring basis, one time services will be handled via a Letter Estimate.

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 Office.

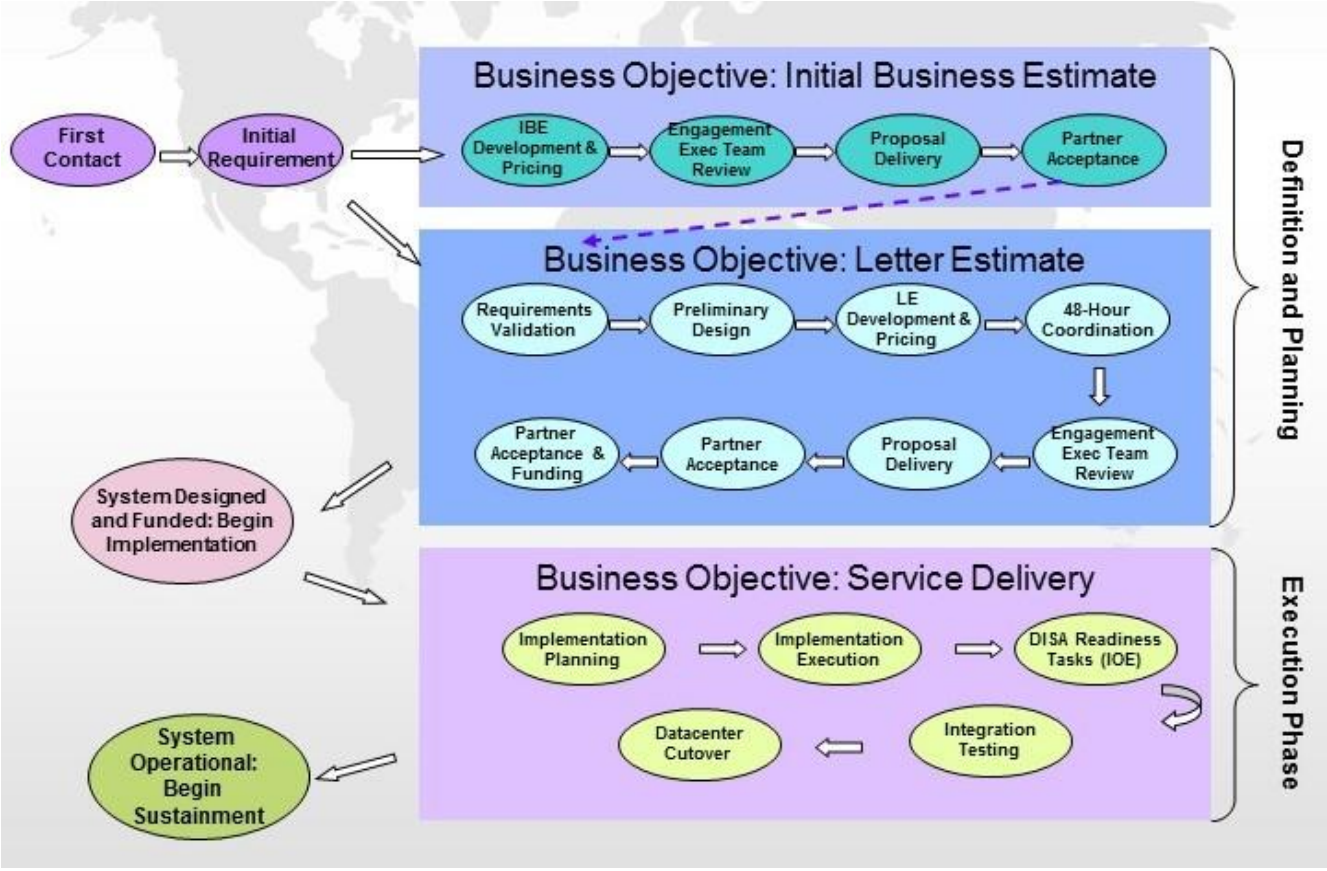
NOTE: milCloud Infrastructure as a Service (IaaS) does not require an LE, SLA, or PE and operates under its own terms and conditions. The full terms and conditions for milCloud IaaS self-service virtual data centers (VDCs) can be found by accessing the Cloud Services Marketplace at https://milcloud.mil.

2.0 Onboarding Paths

The DISA Requirements Management Process (DRMP) fulfillment process governs the project workflow for new partner Computing and Enterprise Services workloads hosted by DISA and any changes to those workloads. The DRMP 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) DRMP 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 the Computing Ecosystem on behalf of the partner
   d) DISA-managed VDC
   e) milCloud optional services (e.g., system and database administration)

3.0 Business Estimate Process



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 5 business days following the agreement of requirements (Functional Baseline), development of the required technical documentation, and submission of the estimate request to the Estimate Writers Team. 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. The overall target timeline to complete the LE is 30 business days. This includes 20 business days to develop the technical documentation following the agreement of requirements (Functional Baseline), and 5 business days to develop the LE following the completion of the technical documentation and submission of the estimate request to the Estimate Writers Team.

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 Mission Partner Engagement Office 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 Office) 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 rate-based Office of the Secretary of Defense [OSD]-approved partner billing rate and reimbursable cost of services prices. Outcomes include an IBE, pricing entry, and a tracking system update.

d) Engagement Office or Division Review – All IBEs shall be reviewed at the Engagement Office-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 Office) 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 rate-based and reimbursable 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 Office or Division Review – All LEs shall be reviewed at the Engagement Office 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 managed within the Computing Ecosystem:

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.
   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 severable services 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 non-severable 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 severable services.
2) New DISA Partner – Upon signature of an LE, the partner must submit funding for non-severable 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.

5.0 Funding and Billing

1) At the beginning of the FY, funding is required during the 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 Defense Working Capital Fund (DWCF) MIPR must contain the following:

   - DISA EIS is a Defense Working Capital Fund (DWCF) and Fee-For-Service (FFS) DoD service provider.
   - As a result, DISA EIS only accepts Category I reimbursable funds
   - DISA EIS "DOES NOT" accept Category II or Direct Cite funds
   - Customer MIPRs should be emailed to the DISA EIS Centralized MIPR mailbox (only): disa.pensacola-fmlo.eis.mbx.pen-miprmail@mail.mil
   - Include the following information in the email Subject line: FY** DoD Service (e.g., Army, Navy, etc.) or Agency (e.g., DLA, DFAS, etc.)_MIPR#_MIPR Sequence (Basic, Amd01, etc.)
     - -e.g.,FY18 AIR FORCE_"MIPR NUMBER"_BASIC
     - -e.g.,FY18 DLA_"MIPR NUMBER"_AMD 01
   - Block 7 of the DD Form 448 (MIPR) should read:
     - DISA Enterprise Information Services
       Attn: RM3212 Revenue Team
       45A Industrial Blvd
       Pensacola, FL 32503
   - Include the following order information in Block 9: Customers should include their DISA EIS Service Level Agreement (SLA) # or Letter Estimate (LE) #, Billing Account Numbers (BANs) and Project Name. Additionally the MIPR should include the appropriate FMR language identifying the type of order the funds support (severable for recurring services or non-severable for implementation). MPs should when available list their financial and technical points-of-contact (TPOCs and FPOCs). Avoid restrictive language by distinguishing between "obligation" authority and Period-of-Performance (POP) dates. POP represents the period in which services will be provided. Typically that would include the fiscal year of issuance (1 Oct **** to 30 Sep ****).
   - If required, MIPRs can be faxed to: (DSN) 459-7567 (comm: 850-452-7567).

- Appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law (ref 31 USC 1301).
- This means unless otherwise specifically stated in the appropriation language, the use of the funds must be used in accordance with the guidelines defined for the general purpose of that type of appropriation.

- Severable MIPR Required Language Block 9:

    - MIPRs in support of recurring services MUST have the appropriate FMR language within Block 9 of the MIPR to be accepted and a 448-2 processed. This mandatory requirement is in support of OSD, the FMR and possible future audits. MIPRs that do not have the required language will be sent back to customers for correction. Required language must also include the Period of Performance (POP).

- Non-Severable MIPR Required Language Block 9:

    - MIPRs in support of non-severable services MUST have the appropriate language within Block 9 of the MIPR to be accepted and a 448-2 processed. This mandatory requirement is in support of OSD, the FMR and possible future audits. MIPRs that do not have the required language will be sent back to customers for correction. Required language must also include the Estimated Project Completion Date (EPCD).

- If a Billing Account Number (BAN) is being funded with multiple DoDAACs, the following verbiage should be included in the body of the MIPR:
- Funds are being provided by Mission Partner end users. The Mission Partner has full responsibility of funding these efforts if any of the following end users default on payments to DISA.
- The below Commands/Agencies will be sending funds:
- (enter DoDAAC) - (enter Command/Agency name) - (enter applicable %)
- (enter DoDAAC) - (enter Command/Agency name) - (enter applicable %)
- (enter DoDAAC) - (enter Command/Agency name) - (enter applicable %)
- These percentages are for (enter current FY) only and the Mission Partner will update these every year, if applicable.
- Mission Partner end users should include the following statement in their MIPR:
- Funds are being provided for SLA # (enter SLA#). This amount represents X% of the PE value.

2) 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.

3) 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.

4) Server and Storage –
   - The severable 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 non-severable 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, raw storage and basic services support 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 calendar 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 Computing Ecosystem 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 Non-secure IP Router Network (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 five distinct processor hardware platforms in DISA:

      - Itanium-based servers from Hewlett-Packard Enterprise (HPE)
      - Power7-based servers from IBM
      - Mainframe systems from IBM and Unisys
      - x86-based servers from HPE
      - SPARC-based servers from Oracle

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

DISA uses virtualization technology for server workload. In the x86 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 multiple physical servers into a resource pool where workloads can use resources on the fly; and High Availability (HA) which allows a VM to be started on another physical host automatically in the case of a hardware failure.

In the UNIX space, virtualization and vendor partitioning methods are varied, but the following is a basic description: A single server can support multiple virtual machines (VMs), each with multiple, virtual CPUs, and I/O devices, each generally running separate operating system instances with different OS versions, applications, and users. As a result, each virtual machine can host its own applications in a fully isolated environment. The physical resources of the server are shared amongst any of the virtual machines it hosts.

b) Storage – flash and traditional spinning disk are the primary storage technologies used to support all OSs.

- Flash and traditional spinning disk technologies are used to hold databases, data warehouses, and flat files where immediate access to the data is necessary.
- Deduplicated disk replicated offsite 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 fiber channel connected virtual tape libraries with offsite replication to support the data backup and archiving process.

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 four standalone networks (production, out-of-band [OOB]/EBN, data replication), 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.

ii. OOB/EBN – 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. The EBN, as described above, employs a high speed IP-based network connecting workloads to automatic tape libraries to support the data backup and archiving process.

iii. Data Replication – This network is comprised of point-to-point circuits between Computing Ecosystem Datacenters locations. It provides secure, IP-based network transport for SAN, mainframe, tape, and host-based replication.

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, HPE Itanium servers, HPE x86 servers, and communications hardware.

   DISA is responsible for all DISA-owned equipment within the Computing Ecosystem Datacenters. Annual inventories include all equipment in the Datacenters; 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 Datacenters 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 calendar 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 licenses. 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 when required.

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, as defined in these T&Cs, 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 **Standard Hosting Services**:
    a) DISA and partners will adhere to the below in the management of their traditional security and cybersecurity programs:
        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 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, United States Cyber Command (USCYBERCOM), Joint Forces Headquarters-Department of Defense Information Network (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 Service Providers (CSSPs) 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.

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, and 3 .

xiv) Abide by RMF reciprocity instructions IAW DoDI 8510.01 Enclosure 5

xv) 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).

xvi) 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]).

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

xviii) Ensure NIPRNet and Secret IP Router Network (SIPRNet) information systems are registered and use Enterprise Mission Assurance Support Service (eMASS) for RMF processes and packages to request and receive automated inheritance from DISA.

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

xx) 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.

xxi) 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) Maintain valid RMF authorization decisions signed by the DISA AO for DISA information systems and applications in implementation and sustainment.

ii) Maintain DISA RMF Service Product assess only packages in support of Partners.

iii) Maintain the following RMF common control packages in eMASS:

(1) **DISA Datacenter (Facility) Packages –** These are assessed and authorized packages which contain "common" physical and environmental controls for inheritance by DISA and Partners who have programs and systems hosted within DISA Datacenters and field activities. These packages are authorized by the DISA Authorizing Official (AO). The eMASS packages format title is Datacenter "Datacenter Name" (ex: Datacenter Montgomery).

(2) **DISA Network Package –** This is an assessed and authorized package which contains "common" transport and network infrastructure controls available for inheritance by DISA and customers who utilize the DISA Computing Ecosystem Command Circuit Service Designators (CCSDs) to transport and receive program and system information. This package is authorized by the DISA AO. The eMASS package titles are EIBN (NIPRNet) and EIBN-C (SIPRNet).

(3) Confidentiality, Integrity, and Availability (CIA) impact levels for Datacenter (Facility) and Network packages are:

Datacenter	NIPRNet	SIPRNet
Confidentiality	High	High
Integrity	Moderate	Moderate
Availability	High	High

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

iv) Maintain the following assess only packages in eMASS:

(1) **DISA Inherited Policy (DIP) Package –** This is an assess only package which contains DoD Chief Information Officer (CIO) and DISA policy/guidance controls assessed and validated as "common" and/or "shared" between DISA and the mission partner. The RMF eMASS package title is DIP-RMF. This package has no CIA.

(2) **DISA Service Product Packages –** These are assess only packages which are comprised of comprehensive security test and/or assessment results for reuse by leveraging organizations, giving its own AO a holistic view of their associated information systems' risk posture.

(a) There are currently five packages defined equating to the level of services desired by the mission partner. Each package contains Control Correlation Identifier (CCIs) assessed and validated as "inherited" and/or "shared" between DISA and the mission partner. These packages are assessed and validated by the DISA Security Control Assessor (SCA). There are no limitations on CIA and all overlays are applied, to include FISCAM. In the near future, package 1 will be merged with package 2 as the CCIs offered are the same. Partners currently assigned to the legacy package 1 will be notified when the changes will occur and DISA will work with them to smoothly transition to the new package.

(b) The eMASS service product package titles and descriptions are listed in the following table. Click on the title link to view a list of inherited/shared controls and CCIs for each package.

(c) Provide inheritable and shared CCIs based on purchased services. The Mission Partner Integration Team will work with the Partner to ensure RMF request form selections are accurate based on the SLA, LE, SRF or other agreements between DISA and our Partner for purchased services.

TITLE (click on package title to view doc)	DESCRIPTION
DISA RMF – Service Package 2	DISA Managed OS Only or OS w/partial Application Management – MP Approval Required
DISA RMF – Service Package 3	DISA Managed OS and all Application Management – MP Approval Required
DISA RMF – Service Package 4	DISA Managed OS Only – Secure At Will
DISA RMF – Service Package 5	DISA Managed OS and all Application – Secure At Will
DISA RMF – Capacity Services	Partner program is on Capacity Services equipment
DISA RMF – COOP	Partner has purchased COOP services
DISA RMF – CSSP	Partner has purchased CSSP services
DISA RMF – Hosted	Partner program is wholly hosted (to include COOP if purchased) in a DISA facility
DISA RMF – Maintenance	Partner has purchased DISA maintenance on partner owned equipment

DISA RMF – Scan	Inheritable/shared controls for HBSS and ACAS services

Function	Package 2 OS Only or OS + Partial Application	Package 3 Entire Application	Package 4 OS Only (VOE only)	Package 5 Entire Application (VOE only)
DISA Responsibility	Manage OS Only or OS & one other platform	Manages OS & All Platforms	Manages OS Only (customer directed configurations)	Manages OS & All Platforms (customer directed configurations)
Patch Management	No authority to patch at will; PM approves	No authority to patch at will; PM approves	DISA Secures at will	DISA Secures at will
Control Responsibility (leans towards)	Controls Shared	Controls Shared	Controls Inheritable or Shared	Controls Inheritable or Shared
Authorization Strategy	Assess Only	Assess Only	Assess Only	Assess Only
Authorizing Official	MP	MP	MP	MP

v) Grant RMF inheritance via eMASS IAW RMF controls spreadsheet.

vi) Make available evidentiary information for reuse by another separate organizations to support a new authorization in order to save time and resources. Reuse is a form of reciprocity because it relies on acceptance of assessment and testing conducted by the DISA SCA

vii) Enforce reciprocity which is a mutual agreement among participating enterprises and an acceptance of each other's security assessments in order to reuse information system resources and/or acceptance of each other's assessed security posture in order to share information. . Evidence will be reviewed annually and updated at that time. No additional artifacts will be provided between reviews unless otherwise agreed upon.

viii) Prohibit retesting of RMF common control provider and assess only results unless agreed upon by all parties through written correspondence.

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

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

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

xii) 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.

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

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

xv) 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.

xvi) 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.

xvii) 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 partner administrative privileges to the underlying OE.

(8) CoN application will not require partner 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

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

xix) Enforce privileged account requirements as outlined in "Privileged Access Guidelines for Ecosystem Managed Systems".

NOTE: To access the Privileged Access Guidelines for Ecosystem Managed Systems document, 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.

xx) Be responsible for quarterly reporting of DISA Computing Ecosystem privileged user accounts for all managed systems, IAW USCYBERCOM Taskord 14-0185 Insider Threat Mitigation.

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

xxii) Authorize and enable full root access to production information systems only when applications are moved to T&D environments, unless agreed to and documented by DISA and Partners.

xxiii) Revoke root access prior to information system promotion into a DISA production environment, unless agreed to and documented by DISA and Partners.

c) Partners will:

i) Update and maintain valid RMF 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 responsible for acquiring and maintaining an account in the Enterprise Security Posture System (ESPS) in order to maintain visibility of the DISA managed security

postures for their program assets. ESPS will be used for creating STIG checklists and pulling security configuration information for RMF CCIs.

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

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

vi) 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.

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

viii) Complete and sign all DD Form 2875 required entries for privileged account requests. Incomplete forms will be returned to the originator for correction. The supervisor's signature will serve as confirmation that the requestor has met all DoD training and certification requirements, has a non-disclosure agreement on file and has a need-to-know for the level of access they are requesting. The cybersecurity professional's signature (ISSO on the current form) will serve as confirmation the requestor has adequate clearance for the system they are requesting access to, and meets the investigation requirements as outlined in the enclosure Privileged Access Guidelines for Ecosystem Managed Systems.

NOTE: To access the Privileged Access Guidelines for Ecosystem Managed Systems document, 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.

ix) Notify Ecosystem of any departures, management reassignments, or other personnel changes where the requestor's access needs to be altered or removed.

x) Maintain access control for users to their applications and maintain copies of DD Form 2875s for active application accounts. Partner will provide the forms to DISA upon request during audits and inspections.

xi) Be responsible for quarterly reporting of Partner privileged user accounts for their programs, in accordance with USCYBERCOM Taskord 14-0185 Insider Threat Mitigation. DISA will report privileged user accounts for all DISA Ecosystem users.

xii) Provide written identification of all CUI, PII, HIPAA, and PCI applications and information being hosted by DISA and ensure compliance with system registration requirements for systems containing privacy act information.

xiii) 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.

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

5) 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.

6) 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 Virtual Data Center (VDC) T&Cs and the VDC Hosting Policy located at https://www.milcloud.mil/.

7) 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 Virtual Machine (VM) managed by DISA.

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

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 full financial statement audit response activities.
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) The Financial Audit Baseline Controls, more specifically the controls for the SSAE-18, 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.
5) DISA and partners shall:
   a) Maintain open communication and coordinate with each other and supporting contractors
   b) Provide additional information and any associated key supporting documentation within agreed upon timeframes
   c) Collaborate to develop a unified plan for achieving and maintaining audit readiness.
6) DISA will:
   a) Prepare for and undergo an annual AT-C 320 examination for IT General Controls.
   b) Prepare for and undergo an annual AT-C320 examination for ATAAPs program/application
   c) Provide applicable financial mission partners with the SOC1 report(s) no later than 15 August of each year.
   d) DISA uses the OUSD FIAR list as the authoritative billing source. Partner application(s) must be identified as hosted at DISA on the list before DISA will start billing.

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.

7) 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) Ensure application/program FISCAM auditors and financial system owners rely on the AT-C 320 SOC1 report to the greatest extent possible.
   c) Evaluate and, as appropriate, implement controls that address the "Complementary Subservice Organization Controls (CSOCs)" as identified in the most recent copy of AT-C 320 report (henceforth referenced as a Service Organization Controls 1 or "SOC1" report) provided by DISA.
   d) Notify DISA of systems hosted within the DISA Computing Ecosystem that are relevant to financial reporting.
   e) Inform DISA of audit and audit readiness activities early in the process in order to properly plan.
   f) Ensure special system requirements are documented and made part of the SLA; for example, include records retention requirements.

8) Audit Support Requests:

   a) Requests for hosting services evidential matter must be submitted on the standard DISA Audit Readiness Request Form located at (https://disa.deps.mil/ext/cop/mpp/docs/srf/compliance-audit-readiness-form.pdf). 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..

   b) 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 onsite in a live session.

   c) 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 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).

12.0 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 test results 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 business 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.

13.0 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	Monthly	Monthly capacity utilization reports for server environments where the partner is paying Hardware Services.
Centralized Invoice System (CIS)	Bi-weekly	Billing amounts charged to MIPRs at the service level.

14.0 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 calendar 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 calendar 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 Office.
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 Office in writing of their intent to decommission two weeks prior to decommission.

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

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

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

5) 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.

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 will be considered a new integration. Beginning in FY17, a new one-time implementation fee will be charged along with an annual recurring fee for the new URL. It is strongly suggested the GCDS PMO is notified at disa.meade.esd.list.gcds@mail.mil prior to taking such action.

6) Shall inform the GCDS PMO anytime a POC responsible for the management of the integrated application changes.

7) Is responsible for maintaining the allocation if the partner uses GCDS NetStorage.

8) 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.

9) 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.

10) Is responsible for the procurement of the broadcast media (camera, hardware or software-based encoder, production equipment).

11) Is responsible for the opening of the required ports on the local firewall to enable the streaming.

12) If using a hardware-based encoder, is responsible for the proper IA authorization and accreditation for using the hardware-based encoder.

13) Is responsible for ensuring the selected media encoder is H.264 Industry Standard compliant.

14) Is responsible for the content and the operational security associated with the streaming event.

15) Shall contact the respective DISA Mission Partner Engagement Office to initiate the request for streaming support.

16) 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
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
CM	Configuration Management

Acronym	Definition
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
CSOC	Complementary Subservice Organization Control
CTO	Communications Task Order
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
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
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency

Acronym	Definition
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
DRMP	DISA Requirements Management Process
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	Fiber 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
GAO	General Accounting Office

Acronym	Definition
GOTS	Government off-the-Shelf
HBA	Host Bus Adapter
HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
HPE	Hewlett-Packard Enterprise
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	Secret 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 calendar 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.
Reciprocity	Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
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.
Reuse	Use of completed security test and/or assessment results made available by a separate organization to support a new authorization in order to save time and resources. The leveraging organization becomes the information system owner and must authorize the system through the complete RMF process, but uses available completed test and assessment results provided by the leveraged organization to the extent possible to support the new authorization by its own AO. Reuse is considered a form of reciprocity because it relies on acceptance of assessment and testing conducted by organizations other than the one authorizing the system in question.

Term	Description
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.
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) DoD FMR 7000.14-R, June 2011
http://comptroller.defense.gov/fmr

7) 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

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

9) 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

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

11) 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

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

13) 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

14) 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

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

16) 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

17) 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

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

19) 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

20) National Defense Authorization Act for Fiscal Year 2017, November 2016
https://www.gpo.gov/fdsys/pkg/CRPT-114hrpt840/pdf/CRPT-114hrpt840.pdf

21) 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

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

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

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

25) 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

26) 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

27) 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

28) 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