Defense Information Systems Agency
The IT Combat Support Agency

Defense Working Capital Fund Billing Prices for Fiscal Year 2018

Effective 1 October 2017

Department of Defense
Defense Information Systems Agency
P.O. Box 549
Ft. Meade, MD 20755-0549

Contents

General Information

This document contains pricing for the FY 2018 DISA services offered on a reimbursable basis through the Defense Working Capital Fund. All prices are effective 01 October 2017 through 30 September 2018. Annual pricing included in this publication is billed at a monthly recurring rate and will be rounded to the nearest cent.

The DISA Implementation and Sustainment POC mailbox is disa.meade.ns.mbx.disn-subscription-service@mail.mil.

This document has been approved for release by the DISA Comptroller. Comptroller POC is Ms. Christina Grant at Commercial 301-225-2291, unclassified e-mail christina.y.grant.civ@mail.mil, and SIPR email christina.y.grant.civ@mail.smil.mil.

Price Book and Order Entry Web Pages

This price book can be found on the Mission Partner Portal under Rate Books in the top navigation bar https://disa.deps.mil/ext/cop/cpp/home.aspx. The order entry website, DISA Storefront, can be accessed at https://disa-storefront.disa.mil/dsf/manage_account/index.

DITCO Contract Service Fee

All DISA telecommunications services are supported by the Defense Information Technology Contracting Organization (DITCO). All pricing in this rate book includes the **2.50%** DITCO contract service fee.

Requirements Not Specified in the Price Book

Pricing for requirements not specified within this publication will be provided by the DISN Program Office once the requirement has been submitted to a DISN provisioning organization, a solution developed, and costs approved by the DISA Comptroller.

DISN Services Frequently Asked Questions

Frequently asked questions regarding DISN services can be found at http://disa.mil/Network-Services/Frequently-Asked-Questions.

Telecommunications Services Billing and Provisioning Points of Contact

The DISA encourages you to work with your Mission Partner Engagement Office (MPEO) point of contact to determine your requirements. Your MPEO POC can be found at http://www.disa.mil/Computing/Engagement-Executive.

For any questions regarding billing, please contact Mission Partner support via one of the email or phone numbers listed below:

Mission Partner	Email	Phone
Air Force	disa.scott.rm.mbx.af-customer-support@mail.mil	(618) 229-9210
Army	disa.scott.rm.mbx.army-customer-support@mail.mil	(618) 229-9591
Navy	disa.scott.rm.mbx.navy-customer-support@mail.mil	(618) 229-9718
Other	disa.scott.rm.mbx.other-customer-support@mail.mil	(618) 229-9519
DISA	disa.scott.rm.mbx.disa-customer-support@mail.mil	(618) 229-9206

For questions regarding the provisioning process of telecommunications services, please contact the DISN Customer Call Center (DCCC):

DCCC	Contact Info
DCCC Service Desk	1-844-DISA-HLP (347-2457), option 2
DCCC Service Desk DSN	312-850-0032, option 2
DCCC Service Desk Email	disa.dccc@mail.mil
DCCC Service Desk Secure Email	disa.scott.conus.mbx.dccc@mail.smil.mil

Telecommunications Services Pricing

TS-DS-01: DISN Infrastructure Services (DISN IS)

The DISN IS includes the transport infrastructure, network operations/management, cyber security, and support services required to provide network services to each Requesting Agency. Analysis of access circuits inventoried in the World-Wide Online System (WWOLS) database was used to determine the allocations of cost. Ordered access circuit capacity is used as a proxy for "usage," and each Requesting Agency is allocated a share of network infrastructure costs based on their percentage of total network capacity (excluding MPLS connections).

An access circuit is defined as a remote access lease connecting a non-DISN node to a DISN Service Delivery Node (SDN). The ordered capacity on these circuits will be used as the basis for each Requesting Agency's DISN IS bill, and Requesting Agencies will continue paying the monthly recurring charges (MRCs) on these leases directly.

DISA Defense Working Capital Fund
Billing Prices for Fiscal Year 2018

DISN IS Cost Allocation, including the 2.50% DITCO fee:

Mission Partner	Sum of Mbps	Percent Allocation	Annual Cost	Monthly Recurring Charge (MRC)
DISN Infrastructure Services (DISN IS) Bill by Mission Partner				
Army	422,058	33.8680%	$338,735,737.85	$28,227,978.15
Navy	210,052	16.8556%	$168,583,540.93	$14,048,628.41
Marine Corps	25,753	2.0666%	$20,669,209.78	$1,722,434.15
Air Force	401,622	32.2281%	$322,333,976.30	$26,861,164.69
Advanced Research Projects Agency	1,339	0.1074%	$1,074,655.04	$89,554.59
Defense Commissary Agency	145	0.0116%	$116,374.15	$9,697.84
Defense Contract Audit Agency	577	0.0463%	$463,088.84	$38,590.74
Defense Contract Management Agency	432	0.0347%	$346,714.70	$28,892.89
Defense Finance and Accounting Service	3,392	0.2722%	$2,722,352.43	$226,862.71
Defense Health Agency	30,322	2.4332%	$24,335,840.30	$2,027,986.69
Defense Information Systems Agency	34,838	2.7956%	$27,960,435.39	$2,330,036.28
Defense Logistics Agency	21,754	1.7456%	$17,459,332.16	$1,454,944.35
Defense Media Activity	2,089	0.1676%	$1,676,590.28	$139,715.85
Defense Security Service	708	0.0568%	$568,226.86	$47,352.24
Defense Telephone Service	3	0.0002%	$2,407.74	$200.64
Defense Threat Reduction Agency	4,370	0.3507%	$3,507,275.98	$292,273.00
DoD Education Agency	14	0.0011%	$11,236.12	$936.35
DoD Inspector General	332	0.0266%	$266,456.66	$22,204.72
DoD-SACA	121	0.0097%	$97,112.22	$8,092.68
Joint Chiefs of Staff	47,494	3.8112%	$38,117,749.46	$3,176,479.12
Missile Defense Agency	2,149	0.1724%	$1,724,745.10	$143,728.76
Office of the Secretary of Defense	32,126	2.5779%	$25,783,695.19	$2,148,641.26
White House Communications Agency	2	0.0001%	$1,203.87	$100.33
Canadian Forces Communication System	14	0.0011%	$11,236.12	$936.35
Department of Commerce	56	0.0045%	$44,944.50	$3,745.37
Department of Energy	143	0.0115%	$114,768.98	$9,564.08
Department of Homeland Security	110	0.0088%	$88,283.83	$7,356.99
Department of Justice	356	0.0286%	$285,718.59	$23,809.88
Department of State	1,809	0.1452%	$1,451,867.79	$120,988.98
Drug Enforcement Agency	83	0.0067%	$66,614.17	$5,551.18
Federal Aviation Administration	6	0.0005%	$4,815.48	$401.29
Federal Bureau of Investigation	104	0.0083%	$83,468.35	$6,955.69
National Aeronautics & Space Administration	5	0.0004%	$4,012.90	$334.41
Nuclear Regulatory Commission	2	0.0002%	$1,605.16	$133.76
US Coast Guard	1,659	0.1331%	$1,331,480.74	$110,956.73
US Postal Service	5	0.0004%	$4,012.90	$334.41
Other	140	0.0112%	$112,361.24	$9,363.44
Grand Total	1,246,185	100.0000%	$1,000,163,148.10	$83,346,929.00

Requesting Agencies can enter a Telecommunications Service Request (TSR) for DISN Infrastructure Services by accessing the DISA Storefront at https://disa-storefront.disa.mil/dsf/manage_account/index, where a walkthrough of the ordering process is provided. Requesting Agencies must ensure that a valid Program Designator Code (PDC) is specified with each order. For any questions regarding the billing processes or how to obtain a PDC, please contact your billing support representative.

Requesting Agencies are encouraged to provide a single PDC for each order in DSF to simplify the ordering process; however, if multiple PDCs are required, please notify your billing support representative of the estimated billing amounts against each PDC prior to placing your order.

DISN Legacy Technologies

Asynchronous Transfer Mode (ATM) and Integrated Services Digital Network (ISDN) have been declared obsolete. Requesting Agencies will be billed on a direct reimbursable basis for any new service requests related to ATM or ISDN. The availability of Multi-Protocol Label Switching (MPLS) and Quality of Service (QoS) renders these services obsolete and generally no longer necessary for most DISN users.

Relocation of DISN Equipment

The need to support the global, dynamic, net-centric requirements of the DoD often results in one-time or non-recurring charges (NRCs). Examples of these charges include relocation of equipment; installation removal of circuits and equipment; installation or removal of cryptographic equipment; addressing of power or heating, ventilation, and air conditioning (HVAC) issues; and other non-operating charges. Requirements may come from within DISA or from a Requesting Agency.

If an Agency requires equipment or a circuit connection to be moved, the Requesting Agency will fund all NRCs including applicable fees. Work on these efforts requires payment of NRCs in advance of work commencement. A minimum of 60 days is required to accomplish any relocation. If a request does not provide a 60-day lead time, expedite charges may be applied to the total Requesting Agency's charges, if expediting is feasible.

For service, please contact the DISN Customer Call Center (DCCC) at 1-844-347-2457.

TS-RS-01: Global Video Services (GVS)

GVS ordering information is available on the GVS Portal at https://globalvideoservices.csd.disa.mil/gvs-web. The ordering information provides instructions for requesting a GVS account, contains a link for downloading the GVS Desktop installation file, and provides instructions for registering traditional VTC endpoints, Multipoint Control Units (MCUs), and gatekeepers with GVS.

Pricing for Global Video Services (GVS) is set annually and will be collected manually, based upon the proportion of Multipoint Control Units (MCUs) and room systems aligned to mission partners. Pricing only applies to the connection of traditional VTC equipment to GVS, this includes Room Systems and MCUs. GVS services are available free of charge to individual users via the GVS Desktop App for their desktop/laptop/thin/zero client. GVS-Unclassified (GVS-U) service is offered on NIPRNet. GVS Classified (GVS-C) service is offered on SIPRNet. GVS Allied (GVS-A) service comes with GVS-C at no additional

charge. While the cost for NIPRNet (GVS-U) and the cost for SIPRNet (GVS-C) services are the same, Requesting Agencies must pay a usage fee for each network being utilized.

GVS monthly rates, including the 2.50% DITCO fee:

GVS Annual Allocation by Requesting Agency				
Requesting Agency	Room System Registrations	MCU Registrations	Percentage of GVS System	Annual Cost
Air Force	2,116	100	36.98%	$9,161,414.42
Army	2,646	464	51.90%	$12,857,400.20
DISA	303	67	6.17%	$1,529,658.54
Marine Corps	62	5	1.12%	$276,992.22
Navy	178	51	3.82%	$946,734.61
TOTAL	**5,305**	**687**	**100.00%**	**$24,772,200.00**

Gatekeeper: A gatekeeper is an appliance on an IP network that registers and manages other VTC appliances such as endpoints, MCUs, and gateways. Gatekeepers registered to GVS allow for appliances registered to that gatekeeper (and other appliances registered to GVS) to connect using "video numbers" (E.164) instead of IP addresses.

Room System/Endpoint: An endpoint is an appliance on a network that can connect to GVS Video Teleconferencing (VTC) via Integrated Services Digital Network (ISDN) or Internet Protocol (IP). Endpoints are typically used to provide VTC connection from small, medium, and large conference rooms/centers.

Multipoint Control Unit (MCU) Port: A Multipoint Control Unit is an appliance that manages multiple GVS endpoints at once, coordinates their video data processing functions, and forwards their flow of media streams between them. An MCU port is one conference port in an MCU. An MCU that can support ten simultaneous conferences is considered to have ten conference/MCU ports. Therefore, the monthly rate for an MCU with ten conference ports is ten times the monthly rate for a single MCU port, and the monthly rate for an MCU with 15 conference ports is 15 times the monthly rate for a single MCU port.

GVS User Account: A GVS user account enables users to conduct ad hoc or scheduled desk-to-desk video calls using their normal desktop, laptop, or thin/zero client with the GVS Desktop App installed. Video calls can be point-to-point (2 parties) or multipoint (3+ parties). Video calls include content/desktop sharing and public/private chat capabilities. A GVS-U account requires a CAC. A GVS-C account requires a SIPR token.

GVS Desktop App: The GVS Desktop App is a soft client available for installation on a user's desktop, laptop, or thin/zero client. With the GVS Desktop App, users can connect to other GVS users or to traditional VTC endpoints and MCUs registered with GVS. Users should follow their local process for

installation of the GVS Desktop App. Some Combatant Commands, Services, and Agencies (CC/S/A) preinstall the GVS Desktop App on user's 'workstation'.

GVS Personal Room: A virtual video conference room is automatically created for a user when the user creates a GVS account. A GVS Personal Room acts like a virtual MCU, allowing two or more people to video conference and share content for collaboration.

GVS Public Room: Users can create a virtual video conference room in addition to their GVS Personal Room. A GVS Public Room acts like a virtual MCU, allowing two or more people to video conference and share content for collaboration. GVS Public Rooms can be scheduled in the GVS Event Scheduler, whereas GVS Personal Rooms cannot.

TS-RS-02: Enhanced Mobile Satellite Service (EMSS)

EMSS is a satellite based telephone and data communications service that provides global voice, data and paging services through the DISN EMSS Gateway in Hawaii. The Distributed Tactical Communications System (DTCS), also referred to as "Netted Iridium," supports radios that provide a handheld, over-the-horizon, beyond-line-of-sight, on-the-move communications solution for U.S. troops in remote locations. This push-to-talk radio allows a user to communicate via voice and data with multiple users at the same time.

In 2014, the Department of Defense (DoD) implemented a fixed cost allocation based on the award of a new EMSS Airtime contract that allows Requesting Agencies to access unlimited airtime on an unlimited number of devices at a fixed cost. Pricing is based on a fixed allocation determined at a service enterprise level using the FY 2013 device count and gateway costs. Gateway and Airtime costs have been merged to create a total fixed allocation for all Requesting Agencies. The service enterprise level cost breakout is listed below; DISA will issue a centralized bill at the Service/Agency level for Iridium services. For specific information on "other" categories, please see the paragraph below and contact the Program Management Office. All Requesting Agencies have access to unlimited airtime on an unlimited number of devices, and are encouraged to utilize this capability. Discontinue actions will only be processed if the device is lost, stolen, or damaged. For Requesting Agencies continuing services into FY 2018, the Program Designator Code (PDC) of record will be billed the new rate effective 1 October 2017 unless a new PDC is provided. Requesting Agencies are responsible for providing FY 2018 Lines of Accounting (LOAs) prior to the start of the new fiscal year.

For all Non-DoD Requesting Agencies, an Interagency Agreement (IAA) is a requirement for services. The FMS 7600 forms will be used government-wide. The form is comprised of two sections, FMS 7600A (Agreement / GT&C), which is initiated by the Servicing agency, and FMS 7600B (Order / MIPR equivalent). DISA will not accept a FMS 7600B without an FMS 7600A signed by both Agencies. DISA has a formatted template agreement for the FMS 7600 Part A that has already been approved by our legal team that must be used to draft each final IAA. All Requesting Agencies are required to know their PDC. Please do not contact the DISA finance office on the IAA as their only function is to accept the FMS 7600 Part B once the Part A is signed. For all inquiries, requests and to initiate a FMS 7600 Part A, please contact the DISA EMSS PMO, via email disa.meade.ns.mbx.emss-program-office@mail.mil or phone (301) 225-2800. Timely submission of IAA's by Non-DoD Requesting Agencies is of utmost importance in order for DISA to provide services in a timely manner.

Please note the procurement of devices, and activation fees for new devices/services still apply and are not included in fixed share allocation costs. Activation fees are listed below, and include the 2.50% DITCO fee.

Activation Fees	
Device	**Fee**
Initial SIM Activation	$0.00
SIM Reactivation*	$205.00
Pager	$0.00
Short Burst Data (SBD)	$51.25
DTCS Radio	$51.25
DTCS Net	$51.25

*Only applies to SIMs being reactivated that have previously been deactivated by Requesting Agency.

EMSS Cost Allocation, including the 2.50% DITCO fee:

EMSS Fixed Cost Allocation		
Enterprise Groups	**Percent Allocation**	**FY 2018 Annual Allocation**
Air Force	13.38%	$20,387,241.95
Army	32.77%	$49,929,076.69
DISA	8.45%	$12,870,335.87
Marines	11.00%	$16,756,489.02
Navy	12.94%	$19,719,785.93
NGA	0.25%	$386,807.23
Non DoD	11.66%	$17,762,235.63
Other DoD	7.50%	$11,429,997.58
SOCOM	2.04%	$3,109,930.09
Grand Total	**100.00%**	**$152,351,899.99**

Field Service Representatives (FSRs) will continue to provide logistical, training, and other technical services related to the Iridium satellite-based Distributed Tactical Communications System (DTCS), also known as "netted Iridium." Service will only be provided pending a validated requirement to a DISA contracting officer via a funded Military Interdepartmental Purchase Request (MIPR).

For additional information, please contact:
- EMSS: DISA/EMSS PMO at 301-225-2800 or disa.meade.ns.mbx.emss-program-office@mail.mil
- DTCS: DISA/DTCS PMO at 301-225-2800 or disa.meade.ns.mbx.dtcs-program-office@mail.mil

TS-RS-03: Joint Hawaii Information Transfer System (JHITS) / Pacific Enterprise Service-Hawaii (PES-HI)

JHITS provides the primary inter-and intra-base telecommunications services for the DoD in the State of Hawaii, providing end-to-end common user switched and dedicated transmission services.

JHITS services must be ordered through the JHITS contractor's Communications Information Tool (COMIT) system. Requesting Agencies may also need to submit DISA Storefront Telecommunication Service Request (TSR) requirements for access circuits, i.e., intra-Hawaii tail circuits, so that the TSR is routed to the respective Government provisioning group in Hawaii for processing JHITS service requests (SR) through the COMIT system.

Another method to order JHITS service is via the local Hawaii military Base Communications Officer (BCO) particularly for JHITS telephone services; point-to-point intra-base and inter-base circuits. Requesting Agencies should contact their respective Hawaii BCO for assistance with processing JHITS Service Requests through COMIT. Hawaii BCO contact info is as follows:

- Hawaii Joint Base Pearl Harbor Hickam (JBPHH) Navy Base Communications Officer (BCO), DSN 315-453-0354, Commercial (808) 653-0354
- Hawaii Army BCO, DSN 315-456-1727, Commercial (808) 656-1727
- Hawaii Marines BCO, DSN 315-457-3246, Commercial (808) 257-3246

JHITS monthly billing for switched voice and ISDN service will be charged to all phone numbers serviced by the JHITS switches to include all PBX telephone numbers serviced behind the JHITS switches.

A complete listing of JHITS rates may be found in the JHITS FY 2018 Rates document that is posted on the Mission Partner Portal at URL https://disa.deps.mil/ext/cop/cpp/home.aspx.

Throughout FY 2018, JHITS will be transitioning to the Pacific Enterprise Services - Hawaii (PES-HI). This transition will ensure DISA continues to provide inter-and intra-base telecommunications services for the Department of Defense (DoD) in the State of Hawaii. Further, this transition will continue to provide end-to-end common user switched and dedicated transmission services while aligning the Hawaiian network with broader Departmental objectives and goals. JHITS services will seamlessly transition to PES-HI services and Requesting Agencies will continue to order PES-HI services via COMIT and DSF. DISA will clearly communicate any changes and benefits from PES-HI throughout the transition process.

For additional information on JHITS, contact Ms. Leah Rogers at DSN 375-2532; Commercial 301-225-2532; Unclassified email leah.m.rogers4.civ@mail.mil or CPT Andrea Muncy at DSN 315-472-2200; Commercial 808-472-2200; Unclassified email andrea.p.muncy.mil@mail.mil.

TS-RS-04: Commercial Satellite Services (COMSATCOM)

DISA is the DoD's only authorized service provider for Commercial Satellite Services (COMSATCOM). Additionally, any U.S. and tribal Government organization can utilize this offering, as well as certain foreign entities. DISA is also the COMSATCOM Subject Matter Expert (SME) for the DoD.

Mission Partners purchase their Fixed Satellite Services (FSS) or Inmarsat Mobile Satellite Services (MSS) solution through the DISA SATCOM Division using specially constructed contracts or one of the

DISA/General Services Administration (GSA) contract vehicles available under the Future COMSATCOM Services Acquisition (FCSA) agreements, for emergency, short-term or enduring needs.

The DISA SATCOM Division will work with the Mission Partner to determine the best contract strategy to meet their unique requirements. Some contract mechanisms currently used include:

- Transponded Capacity is generally provided through our FCSA GSA Schedule 70 Special Item Number (SIN) 132-54 contracts, from which almost any increment of bandwidth and power can be acquired in any commercially available frequency band, like L-, S-, C-, X-, Ku-, extended Ku-, Ka-, and Ultra High Frequency (UHF).
- Subscription Services are generally provided through our FCSA GSA Schedule 70 SIN 132-55 contracts, to entail pre-existing or pre-engineered FSS and/or MSS solutions, typically including shared or dedicated satellite resources, ancillary terrestrial components, and contractor specified networks and equipment, in any commercially available COMSATCOM frequency band.
- Blanket Purchase Agreements (BPAs) can be established for FSS or MSS solutions. Two special BPAs exist for FSS solutions: Army TROJAN and Navy X-band On Demand services. Several others exist for MSS solutions: Aeronautical, Agencies BGAN, Air Force BGAN, BSTA, Consolidated BGAN/GX (was Army BGAN), Maritime, Navy/Marines BGAN, SOCOM, and Army TROJAN. Once the BPA is established, Mission Partners place (e.g., MSS) orders through the DISA Storefront system, or via an alternative method approved for that BPA by the SATCOM Division and DITCO.
- Complex Custom SATCOM Solutions (CS3), once available, will replace CS2 and CS2SB to address non-standard, customized engineered offerings by a single provider to meet your unique needs. CS3 will provide complete, customized end-to-end solutions using any combination of FSS and/or MSS, including components and ancillary equipment (e.g., terminals, teleports, terrestrial interface tail circuits, subscriber identity module cards, and peripherals) in any commercially available frequency band, and services (e.g., licensing, integration, installation, testing, network management, engineering, and training). CS3 will offer multifaceted capabilities including, but not limited to: Interactive Services; Continuity of Operations; Broadcast Satellite Services Fleet and Asset Tracking and Reporting Services; Emergency responder operations; Steady State Operations; and Direct Customer Operations.
- Separate unique contracts can be constructed.
- Special situations like emergency need-now actions also happen for which we can check for bandwidth being available through an existing contract with that customer's prior acceptance.

As DISA COMSATCOM is a full services solution provider, and due to the unique nature and broad scope, each acquisition, regardless of type, will be handled contractually independent, and with best practice processes. As well, each requirement must be fully funded by a single or group of Mission Partners.

The total price to the Mission Partner for each requirement is comprised of three elements:
1) **Vendor contract cost** for the requested goods and services
2) COMSATCOM program office **Mission Partner support fee of 2.99%**
3) DITCO **contract service fee of 2.50%**
- The composite fee which accounts for the Mission Partner support fee and the DITCO fee combined is **5.56475%**

The COMSATCOM program office support fee covers DISA's cost for the analysis of and assistance with Mission Partner requirements and alternatives, information assurance regulations compliance,

technical evaluation boards, provisioning and activation of service actions, post award mission support, contracting officer representative (COR) contract monitoring and vendor payment approvals, electromagnetic interference (EMI) and anomaly resolution, contract renewal and modification efforts, plus life cycle acquisition support to the overarching contracts as well as for your individual contact(s), and future considerations like regarding the DoD-wide Analysis of Alternatives and certain Pathfinder actions, plus serving as the program manager and as an advocate for the use of commercial satellite communications in order to ease acquisition, lower costs, and increase the availability and flexibility of commercial and military communications.

The first step in obtaining commercial satellite goods and services is generally to contact the Commercial Cell at your local Regional SATCOM Support Center (RSSC):

- West   CMCL 719-554-0927/4304   DSN 312-692-0927/4304
- East   CMCL 813-828-6836/6841   DSN 312-968-6836/6841
- Europe   CMCL 49 (0)711 907120 5265   DSN 324-434-5230
- Pacific   CMCL 808-656-0683   DSN 315-456-656-0683

For Mission Partners not supported by a RSSC, or for those wanting Administrative or Headquarters support, please contact:

- Mr. Michael A. Nichols at Commercial 301-225-2211, DSN 312-375-2211, or unclassified email at michael.a.nichols16.civ@mail.mil.

For service or assistance specific to MSS, please contact our MSS Help Desk:

- MSS Help Desk at Commercial 301-225-2600, DSN 312-375-2600, or unclassified email disa.meade.ns.mbx.comsatcom-mss@mail.mil.

TS-RS-05: Mission Partner Premise Router Management

Mission Partners of DISA's Internet Protocol Router (IPR) networks may order router management services from DISA. Premise router maintenance is NOT in this service offering. Eligible premise routers include routers which have been approved and accepted by the Joint Interoperability Test Command (JTIC) as a DISN standard. These routers must be directly connected to a DISN hub-router. Router management services include configuration updates, reloads, addressing, and protocol management. Also, remote fault isolation and troubleshooting of the premise router, restoration of hardware equipment, and software configuration are provided. Additional information is available in the "SIPRNet Customer Connection Process Guide" and the "Defense Information System Network Router Network Subscriber Guide" at https://www.nic.mil.

For additional assistance, contact the DISN Customer Call Center (DCCC) at 1-844-347-2457.

DISA will charge the actual cost for providing premise router management services plus the 2.50% contract service fee.

TS-RS-06: Organizational Messaging Service (OMS)

OMS allows for the ability to exchange official information between military organizations and to support interoperability with allied nations, non-DoD activities and the Intelligence Community (IC) operating in both the strategic/fixed-base and the tactical/deployed environments.

OMS Cost Allocation, including the 2.50% DITCO fee:

Organizational Messaging Service Allocation			
Organization	Percent Allocation	FY 2018 Customer Bill	Monthly Recurring Charge (MRC)
Navy (includes assigned COCOMs)	35%	$7,007,822.50	$583,985.21
Air Force (includes assigned COCOMs)	30%	$6,006,705.00	$500,558.75
Army (includes assigned COCOMs)	30%	$6,006,705.00	$500,558.75
DIA (with reimbursement from the Intel Community)	5%	$1,001,117.50	$83,426.46
Grand Total	**100%**	**$20,022,350.00**	**$1,668,529.17**

Requesting Agencies are required to submit a Telecommunication Request (TR) via the DISA Storefront system for revenue collection.

TS-RS-07: Mobility Services

The DoD Mobility Program provides enterprise-level Unclassified and Classified mobile communications services which ensure interoperability, increased security, and access to information. The Mobility Program utilizes Commercial Mobile Devices (CMDs) and commercial carrier infrastructure, coupled with the DWCF enterprise mobility infrastructure service, to provide DoD requesting agencies with access to classified and unclassified data on mobile devices.

DoD Mobility Unclassified Capability (DMUC)

DMUC is an enterprise service that provisions, manages, and protects unclassified mobile access to the Department of Defense Information Network (DODIN). DMUC leverages commercial technology and products to the greatest extent possible while allowing broad access to enterprise services, such as Defense Enterprise Email (DEE), to provide a seamless user experience between desktop and mobile environments. Requesting Agencies, consisting of organizations within the various Combatant Commands, Services, and Agencies (CC/S/A) no longer need to develop, implement, and manage the technical infrastructure needed to connect commercial mobile devices (CMDs) to the Defense Information System Network (DISN).

DMUC service offers:
- Device management through a Mobile Device Manager (MDM)
- Secure container that supports DoD Enterprise Email (DEE) with S/MIME for encrypting, unencrypting, and signing email
- Secure FOUO contacts, calendar, and secure browser
- Access to DoD-controlled Mobile Application Store (MAS)
- Access to NIPRNET
- Level 2 and Level 3 service desks
- Net assurance
- Level 1 service desk training

DMUC Requesting Agency responsibilities include:

- Purchase of approved devices through an organizationally (non-DISA) approved procurement method
- Purchase of cellular service (if desired) through an organizationally (non- DISA) approved procurement method
- Purchase of DWCF Mobility Infrastructure Service through DISA Storefront
- Level 1 Help Desk

DoD Mobility Classified Capability (DMCC)

DMCC is an enterprise service that provisions, manages, and protects classified mobile access to the Secret Internet Protocol Router Network (SIPRNet). DMCC leverages commercial technology and products to the greatest extent possible while allowing access to SIPRNet email and secure voice communications via a secure VOIP capability. Bringing these capabilities to a mobile device allows CC/S/As greater flexibility in secure communications.

DMCC Service offers:
- SIPR connection
- Access to SIPR DoD Enterprise Email
- Voice over internet protocol service
- Level 2 and Level 3 service desk support
- Net Assurance
- Training for Level 1 service personnel

DMCC Requesting Agency responsibilities include:
- Purchase of a DISA-approved mobile device
- Purchase of DISA-approved cellular service
- Purchase of DWCF Mobility Infrastructure Service through DISA Storefront
- Level 1 Help Desk
- Wi-Fi hotspot for international use (Mandatory)

Billing Information

Billing will occur at the end of the month and monthly recurring charges for Mobility services are not pro-rated within a given month. The billing effective date will be the date the Mobility PMO approves the order, which will occur after the requesting organization submits an order in the DISA Storefront portal. Orders will carry over from year to year and may be discontinued at any time.

Monthly Mobility rates, including the 2.50% DITCO fee:

Monthly Mobility Rates by Device Type	
DoD Mobility Program Service	FY 2018 Monthly Rates
DMUC	$4.31 per device per month
DMCC Secret	$59.05 per device per month

Please note all Requesting Agencies must have the approval of the Mobility Program Office prior to submission of orders. This restriction is due to necessary pre-configuration of organizational

requirements in the MDM. Any orders placed in DDSF without the prior approval of the Mobility PMO will be disapproved.

For assistance with obtaining more information on how to join the Mobility Program, please contact your CC/S/A's Mobility Liaison Officer (LNO). If your CC/S/A does not have an LNO, please contact disa.meade.cae.mbx.dod-mobility-outreach-team@mail.mil.

For more information on Mobility-approved devices, mobile applications, the Mobility Program, and more, please visit the Mobility Program website: http://www.disa.mil/Services/Enterprise-Services/Mobility.

TS-RS-08: Cross Domain Services (CDS)

Reimbursable CDS includes Enterprise Hosted Structured File Transfer and Enterprise Hosted Web Service functions. Services related to Enterprise Cross Domain Email and Enterprise Cross Domain File Sharing are included as part of the DISN Subscription Services.

Pricing for reimbursable CDS is separated into three categories: a new filter development fee, a pre/post deployment fee, and a monthly service fee.

The fees for new filter development and new pre/post deployment are based on the cost to develop, certify, and deploy new filters for Structured File Transfer and Web Service functions. Development is a one-time fee per new filter, and pre/post deployment is a one-time fee per each new Requesting Agency. Complex requirements may receive custom pricing to recover the incremental costs.

The monthly service fee covers cross domain technology assessment, security policy enforcement, certification, accreditation and revalidation support, configuration management, help desk support, and life cycle replacement. The monthly service fee is applied as soon as a requirement is declared operational.

Cross Domain Services rates, including the 2.50% DITCO fee:

Cross Domain Services Rates	
Service Offering	**FY 2018 Rates**
New Filter Implementation	$183,986.48 per new filter
Monthly Sustainment	$6,149.49 per filter per month

Requesting Agencies are required to submit a DD Form 448, Military Interdepartmental Purchase Request (MIPR) for revenue collection. For service or assistance, please contact the Cross Domain Services Business Office, Roger Colón, at Commercial 301-225-8531, DSN: 375-8531, or unclassified email roger.colon1.civ@mail.mil.

Cyber Security General Information

A. In accordance with DWCF policy, customers are required to place orders and provide payment for DISA services. Prices for these services are provided in Sections 2, 3, 4 and 5 of this document, and customer MIPR instructions are provided in Section 6.

Per FMR Volume 11B, Chapter 11, "customer orders (funded requests for goods or services) provide the budgetary and cash resources necessary to finance operations [of a DWCF business entity]. . . . A DWCF business entity shall not initiate work or services or incur obligations until customer orders are signed and advanced funding is received." Therefore, DISA requires upfront funding documents for services in FY 2017.

B. DISA encourages you to work with your Mission Partner Engagement Office (MPEO) Point of Contact to determine your requirements.

C. All RME and DRSI services are supported by the Defense Information Technology Contracting Organization (DITCO), therefore the 2.5% DITCO contract service fee is an added amount to customer bills.

CDSP Subscription Services

CDSP Subscription Services Overview

DoDI 8530.01 requires all DoD and non-DoD networks connecting to the Defense Information Systems Network (DISN) to align with an accredited Tier 2 Cyberspace Defense Service Provider (CDSP), previously Computer Network Defense Service Provider (CNDSP). Customers will receive year-long support with the purchase of any of the services described in this section, unless specified otherwise.

TS-CS-01: Required CDSP Subscription Services

1.   CDSP Subscription Services:
    i.   *Malware Notification Protection* - The processes by which the CDSP alerts Subscribers to new malware and assists the Subscriber when an incident occurs. The CDSP maintains contact with Anti-Malware software vendors so that effective countermeasures are developed, tested, and deployed as quickly as possible.

    ii.   *Subscriber Support and IA Training (S&T)* - Includes the includes the coordination of the initial request for services, support agreements and funding, maintenance of Subscriber configuration information, coordination and de-confliction of external assessments, and CDSP programmatic sustainment activities. This also includes high-level coordination and support for CDSP Subscriber Cybersecurity training requirements to include: providing assistance in acquiring Cybersecurity education and training, and spreading knowledge and awareness throughout DoD.

    iii.   *INFOCON Compliance/NETOPS Awareness (INFOCON*) - involves the monitoring of the CDSP Subscriber's INFOCON level, providing technical subject matter experts (SMEs) to the commander, as requested, to assist with determining INFOCON/CPCON measures, and tracking and reporting INFOCON/CPCON compliance.

    iv.   *Information Assurance Vulnerability Management (IAVM)* - USCYBERCOM directly alerts all Combatant Commands, Services, DoD Agencies and Field Activities of new/emerging threats and vulnerabilities. DISA manages the IAVM system for DoD. DISA's CDSP program can provide Subscriber support and facilitate communication with component IAVM SMEs for IAVM implementation and compliance support.

    v.   *Attack Sensing and Warning (ASW)* - collection, normalization, and correlation of event incident data to identify intentional unauthorized activity across a large spectrum, including computer intrusions or attacks, coupled with the

notification to Command and Control and decision makers in order to develop an appropriate response. AS&W senses changes in Subscriber computer networks based on the analysis of current and archived security information. This data comes from all available sources including but not limited to: device logs, security application logs, incident tickets, archives, etc. Data from other CDSPs and Subscribers is correlated to provide more comprehensive AS&W. This type of analysis requires highly skilled Defensive Cyber Operations (DCO) analysts and hinges on collaboration with all stakeholders in the CD hierarchy.

vi.   *Warning Intelligence (WI) or Indications and Warning (I&W)* - Intelligence- based activities that are intended to detect and report on time-sensitive intelligence information on foreign developments that could involve a threat to the United States military, political, or economic interests. I&W provides information on adversaries and

includes forewarnings of enemy actions or intentions. The relevant I&W information relating to DoD information systems and computer networks received from USSTRATCOM or other intelligence sources is distributed to Subscribers for situational awareness.

vii.   *Incident Reporting* - Utilizes an incident reporting system for complete and meaningful incident report recording and rapid distribution to DoD channels and law enforcement/intelligence communities. This involves both up channel (to USCYBERCOM) reporting on behalf of the Subscriber and down-channel (to Subscriber) reporting for recovery and response actions. This additionally involves the filing and safeguarding of all incident reports so that valuable information is available for current and future analysis.

viii.   *Incident Response Support – (IRRT)* - Used to determine the effect of incidents on subscriber networks to prevent further damage and aid in the recovery process. Each mission focuses on identification of system compromises, remediation, and prevention. This service can consist of five missions:

1.   **Volatile Data Analysis (VDA)** is the rapid analysis of a subset of data collected from a system suspected of being compromised, to include RAM and other volatile data. The limited data allows for a greatly reduced timeline in determining a system's integrity.

2.   **Forensic Media Analysis (FMA)** is the analysis of media (hard drives, mobile devices, etc.) to determine their integrity through community derived forensics standards. FMAs are typically conducted when a system is suspected of compromise and VDAs are insufficient in determining the system's integrity.

3.   **Reverse Engineering and Malware Analysis (RE/MA)** is the analysis of executable files to determine their purpose, capabilities, detection mechanisms,

and/or preventative measures. Analysis levels vary from triage to full reverse engineering, depending on the sample.

4. **Intrusion Assessment (IA)** is synonymous with hunting. To accomplish this goal, IRRT deploys to a customer location for a planned, proactive assessment of customer networks to search for any unknown system compromises.

5. **Incident Response (IR)** is the rapid deployment of the IRRT to a Subscriber's location to counter a known, uncontained threat. During the deployment, IRRT hunts for all malicious activity, quarantines the threat, and restores the integrity of the customer's network.

CDSP Subscription Services Rate: **$48,120 per customer, per year.**

2. Network Security Monitoring/Intrusion Detection includes the monitoring of sensors that detect attacks on the DoDIN. This is accomplished through the monitoring of Subscriber networks to detect unauthorized activity via Intrusion Detection and Prevention Systems (IDPS) and determining if network and host activity is intrusion related. The IDPS-derived information provides analysts with technical event and incident data to process into intrusion analysis, correlation, and reporting. The size of the customer will be determined during the request process.

    i.   Small CDSP Customer: **Rate: $33,588 per sensor, per year.**
    ii.   Medium CDSP Customer: **Rate $38,386 per sensor, per year.**
    iii.   Large CDSP Customer: **Rate $43,184 per sensor, per year.**
    iv.   Extra Large CDSP Customer: **Rate $47,982 per sensor, per year.**

3. Required Vulnerability Analysis and Assessment (VAA) Support Services:
    i.   External Vulnerability Scans (EVS) are conducted in support of, or in augmentation to, the customer's internal, DoD mandated vulnerability scanning and assessment actions. This service is provided primarily for assistance in the protection of a Subscriber's networks and includes:
        1.   Assisting in the execution of external vulnerability scans to determine compliance with DoDI 8551.1 Ports, Protocols, and Services Management (PPSM).
        2.   Providing bi-annual external vulnerability scans of identified targets.
        3.   Recommending vulnerability mitigations and strategies and assist in false positive determination.
        4.   Developing trends and metrics based on available vulnerability data from individual and collective Subscribers.
      The size of the customer will be determined during the request process.

Small CDSP Customer: **Rate: $5,520 per year.**

Medium CDSP Customer: **Rate $6,779 per year.**
Large/Extra Large CDSP Customer: **Rate $8,364 per year.**

ii. Web Vulnerability Scans (WVS) support conducted to assist the Subscriber in complying with USCYBERCOM TASK ORDER 13-0613 with respect to public facing web presence. This service is provided to assist the Subscriber in protecting DoD DMZ Whitelisted web sites and includes:

  1. Semi-annual scans of the Subscriber's public facing websites with follow-on scans for the purpose of validating the Subscriber's mitigation efforts.
  2. Provide web vulnerability testing of all public facing websites in accordance with (IAW) USCYBERCOM TASKORD 13-0613.
  3. Support to all public facing websites registered on the DoD Whitelist and will include all IPs/Fully Qualified Domain Names (FQDNs) to include: public key enabled Common Access Card (CAC), User Identification (USERID) and password, or no access restrictions web listings.
  4. Assistance with false positive determination.

  5. Recommended vulnerability mitigations.

  6. Developing trends and metrics based on available vulnerability data from individual and collective Subscribers.

  The size of the customer will be determined during the request process.

i. Small CDSP Customer: **Rate: $1,218 per year.**
ii. Medium CDSP Customer: **Rate $2,392 per year.**
iii. Large/Extra Large CDSP Customer: **Rate $4,058 per year.**

4. Sustainment and Configuration Management - designed to ensure the assigned Provider continues to provide required CD services to all Subscribers at an acceptable level of quality. A formal agreement, detailing arrangements and expectations between the Provider and each

Subscriber, is key to establishing, measuring, and maintaining a required level of performance. Formal agreements may exist as regulations or instructions within a specific component, but often require explicit SLAs when specific regulatory directives do not exist.

  i. Sensor Deployment and Activation involves the fielding and implementation of CD technologies into the operational environment to support Tier 2 and Tier 3 CDSP.

  Rate $3,680 per sensor (one-time fee)

ii.   Annual Sustainment and CM fee

Rate $500 per sensor/feed, per year.

TS-CS-02: Optional CDSP Services

1.   Vulnerability Analysis and Assessment (VAA) Support Services include:

i.   Penetration Testing is security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. This type of testing is used to determining the effectiveness of the implemented technical security controls, in a goal- oriented, overt manner.

Rate: $3,460 per person per week (plus an additional $3,460 for one week prep/wrap up time).

ii.   Red Team Operation is a focused, threat-based operation by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to develop recommendations for the improvement of the security posture and operational Cybersecurity Defense (CD) capabilities and procedures utilized to protect networks and systems.

Rate: $13,840 per person per month (plus an additional $3,460 for one week prep/wrap up time).

iii.   Intrusion Assessment provides a mechanism for the hunting and eradication of previously unidentified intrusion activity on a network. The end goal of an intrusion assessment is to identify whether a network has been compromised, highlight unauthorized activity, identify any critical vulnerabilities, and provide direction to the customer for the enhancement of local Subscriber cyber defense. Subscribers are entitled to one Intrusion Assessment OR Incident Response per year. Incident Response takes precedence over Intrusion Assessments during scheduling. If an Intrusion Assessment is scheduled and an incident occurs the Intrusion Assessment would be changed to an Incident Response. If an Intrusion Assessment is completed and an incident occurs, the Subscriber will be charged for the subsequent Incident Response, if requested, and will incur a service fee. Additional Incident Response services are charged separately and costs are based on specific requirements.

Rate: $20,760 per assessment

System & Enclave Certification

TS-CS-03: System & Enclave Certification

RME, as a Security Control Assessor (SCA), is responsible to certify customers' internal systems and infrastructure. RME conducts validations of IA/Security posture, determines risk, and develops certification recommendations in support of accreditation for the DISA Authorizing Official (AO). Each accreditation cycle is three years. Customers are charged annually based on the size and complexity of their system/enclave. The sizing parameters are described in Sections 3.B – 3.E.

Small System & Enclave Certification Sampling

- No applications, database, or web (enclave only)
- Administrative network (enclave only)
- One operating system
- No Cross Domain Solutions (CDS) (enclave only)
- One site only

Rate: $15,603 per system, per year.

Medium System & Enclave Certification Sampling

- Two or less applications
- Two or less operating systems
- Less than 300 workstations (enclave only)
- Less than 25 servers (enclave only)
- Up to 2 web servers (enclave only)
- Three or less web instances (system only)
- Up to 2 databases (enclave only)
- Two or less database instances (system only)
- One site only

Rate: $28,439 per system, per year.

Large System & Enclave Certification Sampling

- Any system with a CDS (system only)
- Three - five applications
- More than two operating systems
- 300 or more workstations (enclave only)
- 25-30 servers (enclave only)
- More than three web instances (system only)

- 3-10 databases (enclave only)
- More than one site

Rate: $74,107 per system, per year.

Extra-Large Enterprise System & Enclave Certification Sampling
(any type accreditation system deployed to a DoD enterprise)

- Any system with a CDS (system only)
- More than five applications
- More than two operating systems
- 300 or more workstations (enclave only)
- 50 or more servers (enclave only)
- More than three web instances (system only)
- More than 10 databases (enclave only)
- More than one site
- Two weeks on-site

Rate: $134,124 per system, per year.

Information Assurance (IA) Analysis

IA Analysis Overview

IA Analysis represents a collection of services customers can purchase individually in support of their security and assurance requirements. Rates published represent the average cost of providing these services. Actual charges will depend on the true level of effort needed to complete a particular service.

TS-CS-04: Site Assistance Visits (SAVs)

Site Assistance Visits (SAV) are a process by which DISA Risk Management Executive (RME) personnel will
conduct an on-site assessment of compliance and validation with mandated information assurance (IA), cybersecurity defense (CD), assessment and authorization (A&A), or other focus areas either as a stand-alone effort or in preparation for a scheduled inspection or evaluation. Rates are based per one week SAV as follows:

- 1 Team Lead and 3 Reviewers: $46,808
- 1 Team Lead and 4 Reviewers: $59,664
- 1 Team Lead and 5 Reviewers: $72,481

- 1 Team Lead and 6 Reviewers: $85,317

**Costs will vary if fewer or additional resources are needed.

TS-CS-05: Exercise-Based OPFOR Emulation

Exercise-based OPFOR Emulation service aids customers in assessing their organization's CD posture or
TTP(s).
This service can provide the customer with payload development support, attack execution support, and
penetration and exploitation testing support within the context of exercise or exercise-like events.

Rate: $3,460 per person per week (plus an additional $3,460 for one week prep/wrap up time).

TS-CS-06: Dedicated Team Lead Support

Dedicated Team Lead Support performs Team Lead/Security Control Assessor (SCA) functions on
Certification
Assessments. Certification Assessments may include review of self-assessments and other certification
artifacts and/or leading a team to review a system/enclave where the system/enclave resides. The Team
Lead will follow the Assessment and Authorization (A&A) process guidance and normal procedures of a
Team Lead as outlined by the Government. For each certification assessment, the Team Lead will
prepare a certifier's recommendation, statement of residual risk, and certification assessment briefing
slides.

Rate: $305,000 per person per year.

TS-CS-07: Unique Customer Specific Requests

Unique Customer Specific Requests include contracted efforts not captured in any of the other service
descriptions. These requirements will be estimated per customer and will be billed on a reimbursable
basis.

Rate: Actual cost to provide the capability per requirement.

Cybersecurity Service Assessments

TS-CS-08: Cybersecurity Assessments

Cybersecurity service assessments are a service that, prior to FY15, was provided by DISA Field Security
Operations (FSO). Beginning FY15 this service is provided by the DoDIN Readiness and Security

Inspections (DRSI) Directorate. The DoDIN Readiness and Security Inspections Directorate POC for this service is Mr. Clinton Hackney, 717-267-5855 (DSN570- 5855), Clinton.l.hackney.civ@mail.mil.

Cybersecurity service assessment is an evaluation of DoD Component cybersecurity service providers' (CSSP) services and validation of DoD Component-wide IT asset alignment to and coverage by one or more authorized CSSPs, whether organic or external, IAW with DoDI "Cybersecurity Activities Support to DoDIN

Operations". The assessment is used to measure a CSSP's level of maturity by evaluating established processes and operational capabilities to provide required cybersecurity activities to supported systems and sustain internal cybersecurity operations. A cybersecurity service assessment is also used to verify DoD Component-wide coverage for all required cybersecurity activities, IAW DoDI 8530.01, identify and document gaps and overlaps in coverage and provide recommendations to remediate identified deficiencies and improve cybersecurity operations. As the evaluator for General Services (GENSER) DoD cybersecurity services, DISA DoDIN Readiness and Security Inspections (DRSI) will conduct formal cybersecurity service assessments and provide authorization recommendations to the DoD GENSER Cybersecurity Service Authorizing Official (AO), Unites States Cyber Command (USCYBERCOM). The authorization or formal declaration by the AO authorizes that a cybersecurity service provider operates at a level meeting or exceeding authorization standards, and approved to provide cybersecurity services in accordance with DoDI 8530.01. Cybersecurity service assessments are conducted on a three year cycle unless specific circumstances (e.g. significant deficiencies are identified, identified deficiencies are not remediated within established timelines, significant change to cybersecurity operations or infrastructure, etc.) warrant a sooner out-of-cycle re-assessment.

The Evaluator Scoring Metrics (ESM) serves as the tool by which both DoD Components and cybersecurity service providers will conduct self-assessments and the criteria DISA DRSI will use to conduct formal

cybersecurity service assessments. The ESM is categorized by three major service areas; Protect, Detect, Respond, as well as a fourth area to assess an organizations ability to sustain cybersecurity operations. The applicable assessment criteria within the ESM varies depending on whether a DoD Component is providing that particular cybersecurity function organically (i.e., evaluation criteria) or establish external cybersecurity services by aligning to one or more authorized cybersecurity service providers (i.e., validation criteria). However, the assessment methodology is the same and includes a comprehensive documentation review, extensive interviews, and observation of various process and capability demonstrations.

Cybersecurity service assessments include an evaluation of the following activities:
1. Protect
   i. Vulnerability Assessment and Analysis (VAA)
   ii. Vulnerability Management (VM)
   iii. Malware Protection
   iv. Information Operations Condition (INFOCON)

2. Detect
   i. Information Security Continuous Monitoring (ISCM)

       ii.   Insider Threat
      iii.   Warning Intelligence (WI)

      iv.   Attack Sensing and Warning (AS&W)

3.   Respond
      i.   Cyber Incident Handling

4.   Sustain
      i.   Program Management
      ii.   Personnel
      iii.   Security Administration
      iv.   Service Provider Information Systems

- Small cybersecurity service assessments include DoD Components that are not primary cybersecurity service providers.
  - i. One site
  - ii. One week on-site
  - iii. One week pre-coordination/documentation review
  - iv. One week post assessment wrap-up/report generation

  Rate: $54,897 per assessment.

- Medium cybersecurity service assessments include primary cybersecurity service providers that perform centralized cybersecurity operations from a single location.
  - i. One site
  - ii. One week on-site
  - iii. One week pre-coordination/documentation review
  - iv. One week post assessment wrap-up/report generation

  Rate: $74,884 per assessment.

- Large cybersecurity service assessments include cybersecurity service providers that perform de-centralized cybersecurity operations from multiple locations.
  - i. More than one site
  - ii. Two weeks on-site
  - iii. One week pre-coordination and documentation review
  - iv. One week post assessment wrap-up and report generation

  Rate: $105,156 per assessment.

Customer MIPR Process

MIPR Process Overview

On an annual basis, the Customer will provide DISA with a funding document (DD Form 448, Military Interdepartmental Purchase Request (MIPR), or equivalent) to cover costs for all support provided. DISA FSO will return the Acceptance (DD Form 448-2) to the Customer via the point of contact designated on the DD Form 448.

The Customer understands and agrees that, for all reimbursement provided in each Fiscal Year, the order/obligation document (DD Form 448 (MIPR), or equivalent) shall be provided to DISA at the beginning of the Fiscal Year, unless the Customer requests otherwise in writing and DISA agrees, in writing, to accept reimbursement after that date.

B.   The DISA Business/Trading Partner Network number for these services is: DODHC1008. BPN/TPN numbers for both parties shall be placed on all Interservice, Interagency/Intragovernmental Agreements and all other financial obligation documents for those agreements as per U.S. Dept. of Treasury Finance Manual Bulletin No. 2007-03, OMB Memo M-07-03 and USD Comptroller Memo dated 13 April 2007, subject: Revised Intragovernmental Business Rules. See www.BPN.gov.

C.   Funds must be provided with a DD Form 448 (MIPR), or equivalent, and addressed to the following:

DISA
2300 East Drive
BLDG 3600
Scott AFB, IL 62225-5406

The MIPR MUST include the following verbiage in Block 9: "This is for a DISA action for support identified in the Customer Letter Estimate (CLE) and Service Level Agreement (SLA) FS-17-####."

State, on the MIPR in box 9b, that this support is Severable.

Please send MIPR to disa.chambersburg.eis.list.es243-rm@mail.mil and copy your Customer Account Representative (CAR).

Computing Services General Information

A. In accordance with Defense Working Capital Fund (DWCF) policy, customers are required to place orders and provide payment for DISA services. Prices for these services are provided in Sections 2 thru 6 of this document.

   Per FMR Volume 11B, Chapter 11, "customer orders (funded requests for goods or services) provide the budgetary and cash resources necessary to finance operations [of a DWCF business entity]. . . . A DWCF business entity shall not initiate work or services or incur obligations until customer orders are signed and advanced funding is received." Therefore, DISA requires upfront funding documents for services in FY 2018.

B. DISA encourages you to work with your Mission Partner Engagement Office (MPEO) point of contact to determine your requirements.

C. Computing services are supported by the Defense Information Technology Contracting Organization (DITCO), therefore the 2.5% DITCO contract service fee is included in the below listed rates.

D. There are two classifications of Computing Services rates, stabilized and unstabilized. Service offerings with stabilized rates contain billing rates are set two years in advance and are approved by congress. Stabilized rates can only be adjusted through congressional authority. On an exception basis to help ensure full cost recovery for the working capital fund, unstabilized rates can be adjusted by DISA in the year of execution. The subsequent service offerings with stabilized rates are marked with an asterisk (*).

Section 2
Server Hosting and Hosting Virtualization Services

Server Hosting and Virtualization Services

Overview

The traditional hosted server platform is a managed hosting solution for mission partners that need DISA to provide the labor, hardware, and software required to manage and maintain their server Operating Environments (OEs). Most recurring service offerings fall under the server rates (listed below) and custom non-standard requirements are priced in a full-cost recovery fashion outside of the rate structure.

CS-HV-01: Basic Services

Basic Services is the baseline mandatory service offering which includes the system administration and security administration labor, as well as the hardware and software tools required to monitor and manage the OE. It also includes cost for communications support and infrastructure, Level 2 service desk, and the physical and administrative infrastructure needed to support information technology (IT) service delivery.

The standard rates provide on-site support for five 8-hour shifts weekly (e.g., Monday through Friday from 0800 to 1600 CT), a 2-hour response to emergencies on nights and weekends, and on-site support for the monthly scheduled maintenance window.

Basic Services rates are based on the processing power allocated to the OE and are broken into two categories - virtual OEs and physical OEs.

Virtual OEs – Basic Services Virtual includes all "standard" x86 VOEs (Windows and Linux OSs supported on the VMWare platform) and all Oracle Solaris SPARC LDOMs. Basic Services Virtual – Non Standard includes all other virtual OEs including HP IVMs, AIX PowerVMs, virtual machines (VMs) running on dedicated hosts, and mission partner provided virtualized hardware.

Rates
- **Basic Services Virtual** *(Allocation-based charge driven by the processor count, up to a max of five)*
    - **RATE: $378** * per vCPU or core per month
- **Basic Services Virtual Non Standard** *(Any size, any platform)*
    - **RATE: $1,238** * per OE per month

Physical OEs – This rate category includes all x86 and SPARC physical OEs.

Rates
- ***Basic Services Class 1 Physical*** *(Equal to one (1), up to two (2) sockets per OE)*
  - **RATE: $2,144** * per OE per month
- ***Basic Services Class 2 Physical*** *(Greater than two (2), up to four (4) sockets per OE)*
  - **RATE: $2,865** * per OE per month
- ***Basic Services Class 3 Physical*** *(Itanium - Greater than four (4), up to eight (8) sockets per OE and x86 - Greater than 40 cores per OE)*
  - **RATE: $3,161** * per OE per month

COOP OEs – Dedicated COOP OEs will be billed 50% of the applicable Basic Services charge, which is generated by applying half the workload count to the above rates. For Shared COOP capability there is no Basic Services charge.

CS-HV-02: Hardware Services

Hardware Services is also a mandatory service that is applied when DISA provides the hardware. It includes the cost of the hardware itself, the OS (and any virtualization software, if applicable), standard maintenance, as well as miscellaneous items such as racks and cabling. Also included in the Hardware Services rate is technical refresh on a regular schedule and monthly capacity reports. Capacity reporting at the OE level confirms current processor and memory resource usage trends. Reports are published on the Mission Partner Portal in PowerPoint format.

The following hardware is supported:
- x86-based hardware
  - HP x86 (blades and rack mounted servers)
- UNIX-based hardware
  - Oracle SPARC
  - HP Itanium (non-standard offering)
  - IBM Power7 (non-standard offering)

The following OSs are supported:
- x86-based operating systems (virtualization software, such as VMWare, is also included)
  - Microsoft Windows Server Enterprise Edition
  - Red Hat Enterprise (Linux)
  - SuSE Enterprise Server (Linux)
- UNIX-based operating systems
  - Oracle Solaris
  - HP HP-UX (non-standard offering)
  - IBM AIX (non-standard offering)

Virtual OEs – This rate category includes all x86 VOEs (Windows and Linux OSs supported on the VMWare platform) and all Oracle Solaris SPARC LDOMs

Rates
- **HW Services x86 VOE Processor** *(Allocation-based charge driven by the vCPU count)*
  - **RATE: $74** * per vCPU per month
- **HW Services x86 Virtual Memory** *(Allocation-based charge driven by the GBs of memory)*
  - **RATE: $2.67** * per GB per month
- **HW Services SPARC LDOM Processor** *(Allocation-based charge driven by the core count)*
  - **RATE: $253** * per CORE per month
- **HW Services SPARC Virtual Memory** *(Allocation-based charge driven by the GBs of memory)*
  - **RATE: $4.13** * per GB per month

Physical OEs - These rate categories includes all x86, SPARC, and Itanium physical OEs. They are OE-based workload counts which are driven by the number of OEs required.

Rates
- **HW Services x86 Class 1 Physical** *(1 to 2 sockets per OE)*
  - **RATE: $366** * per OE per month
- **HW Services x86 Class 2 Physical** *(>2 to 4 sockets per OE)*
  - **RATE: $610** * per OE per month
- **HW Services x86 Class 3 Physical** *(>40 cores per OE)*
  - **RATE: $3,780** * per OE per month

- **HW Services SPARC Class 1 Physical** *(1 to 2 sockets per OE)*
  - **RATE: $1,675** * per OE per month
- **HW Services SPARC Class 2 Physical** *(>2 to 4 sockets per OE)*
  - **RATE: $3,357** * per OE per month
- **HW Services SPARC Class 3 Physical** *(>4 to 8 sockets per OE)*
  - **RATE: $8,614** * per OE per month

- **HW Services Itanium Class 1 Physical** *(1 to 2 sockets per OE)*
  - **RATE: $3,015** * per OE per month
- **HW Services Itanium Class 2 Physical** *(>2 to 4 sockets per OE)*
  - **RATE: $4,120** * per OE per month
- **HW Services Itanium Class 3 Physical** *(>4 to 8 sockets per OE)*
  - **RATE: $10,162** * per OE per month

- **HW Services Itanium IVMs** *(Any size)*

- ▪ **RATE: $1,250** per IVM per month

Hardware Services pricing for Continuity of Operations (COOP) / Service Continuity: COOP OEs - Dedicated COOP OEs will be billed 100% of the applicable Hardware Services charge. For Shared COOP capability there is a 25% Hardware Services charge, which is generated by applying a quarter of the workload count to the above rates.

Mission partners requesting non-standard hardware will be charged the vendor cost, plus an infrastructure charge, to ensure full cost recovery.

CS-HV-03: Oracle Database Software

The Oracle Database Software rate covers the maintenance cost of Oracle Database Management System (DBMS) software. Along with Microsoft SQL Server, Oracle DBMS is the most frequently used database application among the DISA mission partner community. For that reason, a specific rate for this software has been developed. Since all of the standard rates cover recurring costs, the license fee for Oracle DBMS (and any other software) is charged as a one-time implementation cost. The cost of other database management systems is considered full cost-reimbursable and is not covered by this rate.

Virtual OEs – There are two separate rate categories including a combined rate for x86 and SPARC VMs and a separate rate for Itanium VMs.

Rates
- *Oracle Database Software x86 & SPARC Virtual* (Allocation-based charge driven by the vCPU or core count)
  - ▪ **RATE: $227** * per vCPU or Core per month
- *Oracle Database Software Itanium Virtual* (Allocation-based charge driven by the core count)
  - ▪ **RATE: $453** * per Core per month

Physical OEs – There are also two separate rate categories including a combined rate for x86 and SPARC physical OEs and a separate rate for Itanium physical OEs.

Rates
- *Oracle Database Software x86 & SPARC Class 1 Physical* (1 to 2 sockets per OE)
  - ▪ **RATE: $2,733** * per OE per month
- *Oracle Database Software x86 & SPARC Class 1 Physical* (>2 to 4 sockets per OE)
  - ▪ **RATE: $5,460** * per OE per month
- *Oracle Database Software x86 & SPARC Class 1 Physical* (SPARC - Greater than four (4), up to eight (8) sockets per OE and x86 - Greater than 40 cores per OE)
  - ▪ **RATE: $8,197** * per OE per month

- ***Oracle Database Software Itanium Class 1 Physical*** *(1 to 2 sockets per OE)*
    - **RATE: $5,470** * per OE per month
- ***Oracle Database Software Itanium Class 1 Physical*** *(>2 to 4 sockets per OE)*
    - **RATE: $10,930** * per OE per month
- ***Oracle Database Software Itanium Class 1 Physical*** *(>4 to 8 sockets per OE)*
    - **RATE: $16,394** * per OE per month

CS-HV-04: Application Support/Web Administration

Application Support and Web Administration are optional services.   The mission partner may elect both, either, or neither as add-ons to Basic Services. Application Support and Web Administration are single rates that can be applied to any OEs, irrespective of the size or type of platform or the number of OEs.

Application Support covers the labor required to maintain and operate the application. It is a broad category and the actual activities performed vary according to each program's unique requirements. The application support activities performed necessitate close coordination between DISA and the mission partner to ensure requirements are met.

Application Support does NOT include the following:
- System Administration (SA), which covers maintenance of the hardware and operating system (OS) and is included in the Basic Services rate
- Database Administration (DBA), which is a separate optional service
- Any application development activities, whether in the initial development/deployment phase or any subsequent spiral

The application support function maintains production application processing at the entire system level, so if there is more than one OE in the system the Application Support rate is applied to all OEs. Put another way, this service provides support for the entire application, not just the OE where the application software is running.   While Application Support, Web Administration, and Database Administration must be selected by the mission partner individually in order for DISA to provide the service, any one of these services satisfies the entire system application support requirement.

Web Administration covers the labor required to configure, secure, and maintain web servers that are integrated into the application on any support OS. If the application uses Microsoft Internet Information Services (IIS), DISA system administrators will install and maintain the static content as part of Basic Services at no additional charge; however, if IIS, or any other web server, is integrated into the application, it must be configured and

secured. These functions will only be performed by DISA if the Web Administration service option is purchased. Web Administration does NOT include content management or web site development or modification.

Optional labor services (DBA, App Supt, and Web Admin) on dedicated COOP OEs need to also be present on the production OE.

If Application Support or Web Administration is required on dedicated COOP OEs:
- The service(s) must be present on the production OE(s)
- The charge is 0.5 / 50% per service (for all new requirements)

Rate
- ***Application Support, also used for Web Administration*** *(Any size, any platform)*
  - **RATE: $947** * per OE or VOE per month

CS-HV-05: Database Administration (DBA)

Database Administration (DBA) is an optional service that includes labor support for the mission partner's database OEs. This rate includes DBA support for standard databases including Oracle DMBS, DB2, SQL Server, MySQL, PostgreSQL and the cost of Oracle DBMS tools (if required). DBA is a single rate that applies to all OEs regardless of size or the specific platform.

If the mission partner does not elect full DBA support and retains responsibility for database administration, DISA still must ensure that all databases comply with DOD security guidelines and are ready for security verification activities.   To assist the mission partner in maintaining security compliance, the DBA Security Only rate is available at 10 percent of the full DBA rate and is mandatory for all mission partner-managed databases. This DBA Security Only service is included in the full DBA rate.
DISA database administrators use Oracle Enterprise Manager (OEM) Grid Control to manage mission partners' Oracle databases. OEM Grid Control is a collection of utilities that automates a variety of time-consuming tasks, allowing the database administrators to be more productive. Mission partners who pay the full DBA rate on their database OEs receive the benefit of these tools. For those mission partners who perform their own database administration, there is a 10% DBA charge for management of the OEM Grid Control software. (This cost is in addition to the Database Administration Security Only rate.) The Oracle Management Packs are licensed on a per OE basis and the license and maintenance is charged directly to the mission partner.

If DBA is required on dedicated COOP OEs:
- The service must be present on the production OE
- The charge is 0.5 / 50% per service (for all new requirements)

If DB Security Only is required on dedicated COOP OEs, the charge is the full 1.0 / 100%.

Rates

- **Database Administration** *(Any size, any platform)*
    - **RATE: $1,586** * per OE or VOE per month
- **Database Administration Security Only** *(Any size, any platform)*
    - **RATE: $158** * per OE or VOE per month

CS-HV-06: 24x7 Services

24x7 Services are available for the three main labor categories - System Administration, Database Administration, and Application Support. These rates cover the cost of providing labor support and technical specialists on-site (vs. on-call) around-the-clock seven days a week (second and third shift). 24x7 rates are applied in addition to the base rates that cover first shift.

All "standard" rates include support from 0800-1600 CT with a two hour call back. If a mission partner requires additional support, 24x7 rates must be applied.

24x7 Services are included for no additional charge on dedicated COOP OEs that have 24x7 Services applied to the production OEs.

Rates

- **24x7 Systems Administration** *(Any size, any platform)*
    - **RATE: $465** per OE or VOE per month
- **24x7 Database Administration** *(Any size, any platform)*
    - **RATE: $2,327** per OE or VOE per month
- **24x7 Application Support** *(Any size, any platform)*
    - **RATE: $2,327** per OE or VOE per month

CS-HV-08: One-Time Implementation Charges

The standard / core implementation charge covers the labor and hardware cost incurred before the application reaches IOE and recurring rate-based billing begins. This is a one-time per OE charge that applies to every system regardless of platform type or size. The labor included in the standard implementation charge recovers the cost for the installers, site system administrators, project managers, as well as storage, communications, and the virtualization teams.

The hardware cost included in the standard implementation charge is two months of the recurring rate-based server and storage cost as priced in the LE. Also included in the

standard implementation charge is the cost for a licensed and data-center qualified electrician to provision power for the new hardware.

Rates
- **Server standard implementation labor charge** *(Any size, any platform)*
    - **RATE: $8,623** per OE or VOE
- **Server standard implementation hardware charge**
    - **RATE: 2 months of recurring HW Services and Storage Services cost**

Non-standard implementation charges (if applicable) include up-front, one-time costs for mission partner unique hardware and software requirements. Common examples would be the license cost of application software and unique communications hardware.

CS-HV-09: Converged Solutions / Enterprise Resource Planning (ERP) Solutions

Basic Services

Converged ERP systems are engineered solutions that are designed to help mission partners consolidate multiple workload in a single environment that has been optimized for performance and availability. They are designed to run business-critical enterprise applications while delivering the highest levels of security, efficiency, cost savings, and performance.

DISAs converged solutions offerings have been customized to support this unique application framework. The upfront and recurring cost for the hardware components is priced based on actual vendor cost, outside-the-rates. However, a Basic Services rate has been created specifically for Oracle SuperCluster (OSC) zones that includes many of the same components as "traditional" Basic Services – system and security administration labor, help desk, and the communication and other datacenter infrastructure.

This new rate for OSC zones, which run on Oracle SPARC hardware, has a single price per virtual OE. Also, there's a dedicated rate for converged systems' x86 VOEs, running on HP CS700X hardware, which are assigned workload units based on the number of allocated vCPUs (up to 5 total units).

Rates
- **Basic Services Converged OSC SPARC** *(Any size zone)*
    - **RATE: $563** per OE per month
- **Basic Services Converged x86** *(Allocation-based charge driven by the vCPU count, up to a max of five)*
    - **RATE: $252** per vCPU per month

Basic Services for other hardware types mirrors the traditional server offerings. For example, physical servers, supporting HANA appliances, are priced based on the size of the provisioned OE. Also, x86 VOEs running on capacity services hardware will be priced using traditional hosted Basic Services and Hardware Services rates.

Converged Systems Storage Backup Service

DISAs converged systems are a provided a backup solution to meet security requirements for backups. The solution is documented as part of the LE, and mission partners are charged a per GB rate based on the amount of capacity backed up. The solution is a backup service, not a "solution" per se. NetBackup media servers perform the backups via NetBackup media agents installed on each OE within the converged system. Backups are de-duplicated and written to storage and replicated to an offsite location.

All backup storage requirements will be priced using the unique converged backup storage rate. All other server optional services are priced using standard rates.

Rate
- ***Converged Backup Storage***
    - **RATE: $0.2500** per GB per month

Implementation Labor Charges

There are also three implementation labor charges that reflect the fact that recent cloning technologies have reduced the number of hours required for implementation activities - particularly for virtual environments. Due to the quantity and standardization of ERP systems, project management labor efficiencies for physical environments have also been realized.

Rates
- ***Server Implementation Converged OSC SPARC Virtual***
    - **RATE: $1,241** per zone one-time
- ***Server Implementation Converged x86 Virtual***
    - **RATE: $4,733** per VOE one-time
- ***Server Implementation Converged Physicals***
    - **RATE: $7,759** per OE one-time

CS-HV-07: Mission Partner Unique / Non-Standard Server Solutions

Non-standard unique mission partner requirements will be charged direct cost reimbursable (vendor cost plus an infrastructure charge) to ensure full cost recovery.

**Section 3
Storage Services**

Storage Services

Overview

Mission partners purchasing server services are offered a wide array of storage offerings that allow DISA to provide the level of service required to meet maximum acceptable data loss and minimum acceptable recovery time for each application.

Rate-based server storage pricing is based on the usable gigabyte (GB) of storage allocated per month and the level of service requested by the partner for data recovery.

CS-SS-01: Enterprise Disk Capacity

Enterprise disk is DISA's standard storage offering and includes all applicable hardware, software, storage engineering and administration, tech refresh, and service desk support. Capacity is provisioned to each OE based on mission partner requirements and maintained by DISA.

Rates
- ***Server Storage Enterprise Disk RAID 5***
  - **RATE: $0.7101** * per usable GB per month
- ***Server Storage Enterprise Disk RAID 10***
  - **RATE: $1.1723** * per usable GB per month

CS-SS-02: Backup Services

Backup service is required on all DISA production applications to include weekly operational backup (one copy onsite, retained four weeks), incremental daily backup (one copy onsite, retained for two weeks), and weekly standard backup (one copy offsite, retained for four weeks). Long term retention or additional application backup requirements can be added on an optional basis.

Rate
- ***Server Storage Backup Service***
  - **RATE: $0.3976** * per usable GB per month

CS-SS-03: Tier 2 Disk Capacity

Tier 2 is an optional service providing slow spinning, low performance disk capacity and should be used only for data that is not frequently accessed.

Rate

- ***Server Storage Tier 2 Disk RAID 5***
  - **RATE: $0.3884** * per usable GB per month

CS-SS-04: Shared COOP Capacity

Shared COOP storage services provide recovery to a remote location using shared storage resources. The recovery time will be five days or less and recovery point seven days or less based on the use of data domain replication.

Rate

- ***Server Storage Shared COOP***
  - **RATE: $0.5914** * per usable GB per month

CS-SS-05: Dedicated COOP Host Replication

Dedicated COOP storage services provide recovery to a remote location using dedicated storage resources. Data is replicated via mission partner purchased Oracle Data Guard (or equivalent) and takes place via the host at both the production and COOP locations. The host must also be backed up at both locations. The recovery time and recovery point are nearly instantaneous.

Rates

- ***Server Storage Enterprise Disk RAID 5***
  - **RATE: $0.7101** * per usable GB per month
- ***Server Storage Enterprise Disk RAID 10***
  - **RATE: $1.1723** * per usable GB per month

CS-SS-06: Dedicated COOP SAN Replication

Dedicated COOP storage services provide recovery to a remote location using dedicated storage resources. Data is replicated via the SAN and is not accessible to COOP servers while replication is taking place. The recovery time and recovery point are eight hours. This rate

covers only the replication itself and must be included with enterprise disk at the COOP location.

Rate

- ***Server Storage Dedicated COOP SAN Replication***
  - **RATE: $1.3344** * per usable GB per month

Section 4
Mainframe Processing and Storage (IBM and Unisys) Services

Mainframe Processing and Storage (IBM and Unisys) Services

Overview

Mainframe hardware is supplied through capacity services contracts. DISA supplies executive software to run mission partner applications and labor to manage execution. In addition, cost-reimbursable services are available as requested by the mission partner.

CS-MP-01: IBM - Processing

DISA will host DoD IBM applications using DISA-provided hardware, operating systems (OSs), and labor.

System Administration (SA)
- IBM technical support which maintains the hardware and OS.

Security
- DISA provides both physical security and Information assurance. DISA's Core Data Centers (CDCs) benefit from the high level of physical security afforded by their location on military installations. DISA also provides a superior information assurance (IA) environment.

Data Communications
- This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our mission partners users around the world to connect to mission partners' data and DISA's computers. Once the request for information leaves the user's locale (base, office building, home, etc.), DISA will handle the traffic and expedite the response back to the user.

Service Desk Support - Level II
- Level II service desk support provides two-hour call-back for emergencies Monday - Friday (0800-1600).

Assured Computing / IT Service Continuity
- Mission partners who purchase IBM mainframe with unclassified processing will receive, at no additional charge, the use of a shared COOP processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will

automatically be assigned to the mission partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our partners will be protected by the COOP / Service Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

Capacity Management
- Capacity reporting is used to monitor and validate system resource trends. DISA collects and retains this usage data to use in the analysis of current and projected resource consumption. With this information, decisions about system capacity changes can be made proactively and economically.

Rates
- **IBM CPU Usage**
    - **RATE: $439.8209** per hour per month
- **IBM ZIIP CPU**
    - **RATE: $404.3433** per hour per month

CS-MP-02: IBM - Storage

Storage in the IBM computing environment consists of disk, tape backup, and the associated communication infrastructure. IBM storage services are currently billed within one cumulative rate that includes disk and tape. DISA now offers, at a reduced rate, long term tape storage for mission partners who are required to keep data for long periods of time. To qualify for this rate the data must be older than 400 days and written to tape.

Rates
- **IBM Storage**
    - **RATE: $0.3263** per GB per day
- **IBM Long Term Storage**
    - **RATE: $0.2176** per GB per day

CS-MP-03: IBM - Optional Features

The following features, available upon request, are cost reimbursable and charged directly to the mission partner, in addition to any costs associated with rate-based services. Optional features include:

Application Support

- This feature applies to our partners' production information systems and databases, not to the processing environment's OS or other executive software. The application support function maintains production processing.

Database Administration (DBA)
- These rates consist of 1) the labor costs of DBA support for any database management systems that run on mainframe and 2) the costs of database management tools that improve their productivity. Access is carefully monitored to ensure partners access only their respective data.

Web Administration
- This feature refers to the labor to administer a web server and its associated software. Web administration does not include creating or designing web sites, nor does it apply to managing content on the web servers.

Dedicated Logical Partition (LPAR) / IBM Mainframe
- When our mission partner's application runs in a shared partition on a mainframe, the mission partner will be charged standard mainframe rates. If the partner requires a dedicated partition on a mainframe or a dedicated mainframe, that service will be a surcharge to compensate for the inefficiencies.

CS-MP-04: IBM Linux on System Z - Processing

Specialty engines on the Integrated Facility for Linux Mainframe allow the mainframe to run Linux workloads. Cost is based on Central Processing Unit (CPU) usage, so this is a true pay-for-what-you-use model. Our partners may be able to reduce their software license costs by having many Linux on System z OEs on very few mainframe engines. If several OEs use the same software (i.e. the Oracle Database Management System), all DISA partners who use that software can share the cost. This eliminates the need for each partner to pay for discrete licenses and maintenance.

Standard Features:

System Administration (SA)
- IBM Linux on System z technical support maintains the hardware and operating system (OS).

Security
- DISA's CDCs benefit from the high level of physical security afforded by their location on military installations. DISA also provides a superior information assurance (IA) environment. In the transition to the DoD IA Certification and Accreditation Process

(DIACAP), DISA has accepted Inherited Controls for a wide range of IA responsibilities and functions.

Data Communications
- This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our mission partners users around the nation and the world to connect to the mission partners data and DISA's computers. Once the request for information leaves the user's locale (base, office building, home, etc.), DISA will handle the traffic and expedite the response back to the user.

Service Desk Support - Level II
- Level II service desk support provides two-hour call-back for emergencies Monday - Friday (0800-1600).

Assured Computing / IT Service Continuity
- Our mission partners who purchase Linux on System z with unclassified processing will receive, at no additional charge if using rate-based billing, the use of a shared Continuity of Operations (COOP) processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will automatically be assigned to the mission partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our mission partners will be protected by the COOP / Service Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

Capacity Management
- Capacity reporting is used to monitor and validate system resource trends. DISA collects and retains this usage data to use in the analysis of current and projected resource consumption. With this information, decisions about system capacity changes can be made proactively and economically.

Rate
- ***IBM LINUX***
  - **RATE: $30.2049** per hour per month

CS-MP-05: IBM Linux on System Z - Storage

Storage in the IBM Linux on System Z computing environment consists of SAN LUNs with backup to tape and the associated communication infrastructure, so existing server storage rates apply to this type of workload.

Applicable Server Storage Rates
- **Server Storage Enterprise Disk RAID 5**
  - **RATE: $0.7101** * per usable GB per month
- **Server Storage Backup Service**
  - **RATE: $0.3976** * per usable GB per month
- **Server Storage Dedicated COOP SAN Replication**
  - **RATE: $1.3344** * per usable GB per month

CS-MP-06: IBM Linux on System Z - Optional Features

The Linux on System Z optional features are the same as the server offerings and are charged the server rates.

Rates
- **Application Support, also used for Web Administration** *(Any size, any platform)*
  - **RATE: $947** * per OE or VOE per month
- **Database Administration** *(Any size, any platform)*
  - **RATE: $1,586** * per OE or VOE per month

CS-MP-07: UNISYS - Processing

DISA will host DoD Unisys applications using DISA-provided hardware, operating systems (OSs), and labor.

Standard Features:

System / Database Administration (SA / DBA)
- Unisys technical support which maintains the hardware and operating system (OS).

Security
- DISA's CDCs benefit from the high level of physical security afforded by their location on military installations. DISA also provides a superior information assurance (IA) environment. In the transition to the DoD IA Risk Management Framework (DIARMF) certification and accreditation process, DISA has accepted Inherited Controls for a wide range of IA responsibilities and functions.

Data Communications
- This covers the communications infrastructure – the hardware, software, firmware, and labor – that allows our mission partners users around the world to connect to the mission partners' data and DISA's computers. Once the request for information

leaves the users locale (i.e. base, office building, home, etc.), DISA will handle the traffic and expedite the response back to the user.

ESM Software
- These are the tools DISA uses to monitor the health and well-being of our partners' information systems and data and to manage problems when, or before, they occur. ESM software alerts DISA when conditions are favorable for problems to occur, so DISA can ensure the appropriate technicians are available to resolve any potential problems before they occur.

Service Desk Support - Level II
- Level II service desk support provides two-hour call-back for emergencies Monday - Friday (0800-1600).

Assured Computing / IT Service Continuity
- Our mission partners who purchase Unisys mainframe with unclassified processing will receive, at no additional charge, the use of a shared COOP processor at a remote site for disaster recovery. In addition, the storage infrastructure required for data replication and utilizing the Assured Computing Environment (ACE) will automatically be assigned to the partner for use at the recovery site. The normal charges for this storage service will apply. The end result is that our partners will be protected by the COOP / Service Continuity program through documented recovery procedures and pre-positioned infrastructure and will automatically gain access to the DISA COOP exercise program.

Capacity Management
- Capacity reporting is used to monitor and validate system resource trends. DISA collects and retains this usage data to use in the analysis of current and projected resource consumption. With this information, decisions about system capacity changes can be made proactively and economically.

Rate
- **Unisys SUPS**
  - **RATE: $17.2535** per hour per month

CS-MP-08: UNISYS - Storage

Storage in the Unisys computing environment consists of tape backup and the associated communication infrastructure. Unisys storage services are currently billed within one cumulative rate that includes disk and tape.

Rate

- *Unisys Storage*
  - **RATE: $21.2917** per GB per day

CS-MP-09: UNISYS - Optional Features

The following features, available upon request, are cost reimbursable and charged directly to the partner, in addition to any costs associated with rate-based services. Optional features include:

Application Support
- This feature applies to our mission partners' production information systems and databases, not to the processing environment's OS or other executive software. The application support function maintains production processing.

Dedicated Logical Partition (LPAR) / Unisys Mainframe
- When our mission partner's application runs in a shared partition on a mainframe, the mission partner will be charged standard mainframe rates. If our partner requires a dedicated partition or an entire dedicated mainframe, that service will be a surcharge to compensate for the inefficiencies.

Section 5
Enterprise Services

CS-ES-01: Department of Defense (DoD) Enterprise Email (DEE)

Overview

Department of Defense (DoD) Enterprise Email (DEE) provides secure cloud-based email to the DoD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries. As an enterprise service, DEE reduces the cost of operations and maintenance by consolidating hardware into DISA's secure CDCs. DEE creates a common platform for the DoD, ensuring agencies can easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse. The technical and functional benefits of DEE include:

- Secure access to your email anywhere, at any time, from any place, whether stationary or mobile
- Coordinating efforts by sharing individual, organizational, and resource calendars across the DoD
- Cost reduction of email by eliminating unnecessary administration and inefficient resource utilization, enabling resources to focus on other priorities
- Replication of data between the CDCs, ensuring communications are secure and available when needed

Mailbox Service Offerings

Multiple options are available to provide the appropriate level of storage to accommodate user requirements on both NIPRNet and SIPRNet.
Rates
- ***Enterprise Email Business*** *(4GB)**, also used for Enterprise Email Basic* *(512MB)*
    - **RATE: $3.28** * per account per month
- ***Enterprise Email Premium*** *(10GB)*
    - **RATE: $10.90** per account per month
- ***Enterprise Email Executive*** *(30GB)*
    - **RATE: $19.64** per account per month
- ***Enterprise Email Senior Executive*** *(50GB)*
    - **RATE: $29.09** per account per month

Transition / Implementation

A one-time cost to on-board mission partners to the DoD Enterprise Email (DEE) service. This service comprises several phases including: Engagement, Service Delivery, Pre-Migration, Migration, Post-Migration and close-out. DISA personnel are also assigned to support Defense Enterprise Provisioning Online (DEPO) configuration, Entitlement Manager Approval process, communication verification, bandwidth analysis, pre-migration support and test user configuration support.

Rate

- ***DEE Transition Level 3***
  - **RATE: $60.00** per account

Mobile Devices

Mobile device service supports the ability to access the user Defense Enterprise Email (DEE) mailbox on both legacy BlackBerry devices as well as the BlackBerry 10 smart-phone capability.

Rate

- ***Enterprise Email Mobile Devices***
  - **RATE: $2.75** * per account per month

Journaling

In order to adhere to legal and regulatory requirements, DEE provides the ability to retain all messages and their attachments sent to and from selected journaled mailboxes. Its primary purpose is to record all email activity regardless of its content, origin or destination. Journaled mailboxes are considered electronic records. Billing is based on the number of gigabytes used for mail storage.

Rate

- ***Enterprise Email Journaling***
  - **RATE: $0.40** * per GB per month

Classified Message Incident (CMI)

A Negligent Discharge of Classified Information (NDCI) occurs when classified information is introduced to a system above the level of classification for which the system is accredited. If a Mission Partner organization causes a NDCI within the DEE, it will be held financially liable.

Rate

- ***Negligent Discharge of Classified Information (NDCI)***
    - **RATE: $2,500** per incident

CS-ES-02: milCloud

Overview

milCloud is a cloud-services product portfolio, managed by the DISA that features an integrated suite of capabilities designed to drive agility into the development, deployment and maintenance of secure DoD applications. milCloud is an Infrastructure as a Service (IaaS) solution that leverages a combination of mature Commercial off the Shelf (COTS) and government developed technology to deliver cloud services tailored to needs of the DoD.

All products in the milCloud portfolio feature the following common cloud services characteristics:
- On-Demand, Self-Service: milCloud consumers can place orders on-demand through web-based self-service tools, configure infrastructure resources where appropriate, and manage their mission application's lifecycle running on those resources without manual intervention from DISA support staff.
- Broad Network Access: All milCloud products and services have network connectivity to the DoD Information Networks (DoDINs), and are configured in accordance with relevant DoD security guidelines and approved protocols.
- Resource Pooling: milCloud resources are pooled such that multiple mission partners consume units from pools provisioned by DISA, enabling efficient use of aggregate resources and greater consumption flexibility.
- Rapid Elasticity: The milCloud portfolio has the ability to expand or contract resource use within virtual resource pools.

Rates
- ***milCloud Base Unit***
    - **RATE: $3.61** per unit per day
- ***milCloud Storage***
    - **RATE: $0.0149** per GB per day
- ***milCloud Backup Storage***
    - **RATE: $0.0095** per GB per day
- ***milCloud Memory***
    - **RATE: $0.73** per 2 GB per day
- ***milCloud Implementation***
    - **RATE: $195.00** per unit

Optional Value-Added Services

milCloud Plus - While milCloud services were initially conceived as an Infrastructure as a Service (IaaS) solution, mission partners recognize that one of DISA's core competencies is datacenter administration. This includes system administration, security administration, operational support (help desk), and system management tool administration. It has become clear that some partners want DISA to provide VDC administration.

To address this need, DISA has created a milCloud version of the Basic Services offering called milCloud Plus. milCloud Plus includes the same OE management services included in the traditional hosting rates, customized for the milCloud service. milCloud Plus pairs the flexibility of the milCloud hardware solution with the comprehensive management capabilities of highly qualified engineers and system administrators.

Rate
- ***milCloud Plus***
  - **RATE: $252** * per vCPU per month

Vulnerability Management - DISA's Vulnerability Management service monitors, detects, and protects against cyber-threats using HBSS, ACAS and other tools. Includes vulnerabilities scans, and setting policies for host based security to protect IT network and programs. This service will be billed on the number of programs utilizing the service and the number of program endpoints.

Rates
- ***Vulnerability Programs***
  - **RATE: $825.01** per Program per month
- ***Vulnerability Endpoints***
  - **RATE: $28.27** per Endpoint per month

Dedicated VPN - provides milCloud mission partners the ability to field and control VPN access to their virtual data center(s)(VDCs). This offering will have two billing components. The first is a one-time implementation fee charged per VDC and is based on the estimated labor cost to set up each VPN. The second component is a monthly usage charge per blocks of five users and essentially recovers the software licensing cost for the service.

Rates
- ***milCloud Dedicated VPN***
  - **RATE: $36.83** per VPN per day
- ***milCloud Dedicated VPN Implementation***
  - **RATE: $277.22** per VPN

Iaas Log View - provides milCloud mission partners the ability to collect, view, and archive Edge Gateway logs. Mission partners who opt to use this service will be billed based on the number of Edge Gateways being utilized.

Rate

- ***milCloud IaaS Log View***
  - **RATE: $24.43** per edge gateway per day

milCloud Premium Engineering – provides Mission Partners direct short term access to a team of milCloud specialists that can provide engineering support for their milCloud implementation and provide Virtual Data Center (VDC) design and configuration expertise. Support levels are based on a monthly allocation of labor hours and are offered in Bronze, Silver and Gold options.

Rates

- ***milCloud Premium Engineering Bronze***
  - **RATE: $1,646** per instance
- ***milCloud Premium Engineering Silver***
  - **RATE: $3,291** per instance
- ***milCloud Premium Engineering Gold***
  - **RATE: $8,229** per instance

milCloud 2.0

Overview

The milCloud 2.0 Phase 1 will establish a commercial infrastructure-as-a-service (Iaas) environment in Department of Defense data centers that will be connected to DoD networks and have unclassified workloads transitioned to and stored in the commercial IaaS solution. These information technology (IT) services will be provided under "pay for usage" concept.

All products in the Cloud Portfolio Services Division feature the following common cloud services characteristics:

- Faster: Streamlined ordering process to save time, money and resources
- Easier: Secure, web-based portal automates provisioning, billing, monitoring and reporting (metrics-based usage metering)
- Cost Competitive: "Pay for usage" eliminates over provisioning, and commercial cloud rates leverages practices seen in the private sector

- Customer Service: 24/7 Customer support - Incident reporting and management system
- Transition: Transition support and subject matter experts available by milCloud Task Order (TO)
- Availability: 99.9%
- Secure: All milCloud products and services have network connectivity to the DoD Information Networks (DoDINs), and are configured in accordance with relevant DoD security guidelines and approved protocols
- SIPRNet: milCloud SIPRNet available FY18

milCloud 2.0 is the next generation, secure, cloud infrastructure for the DoD, with an architecture that is highly available, scales seamlessly, and protects highly sensitive applications (initially authorized to Impact Level 5 with plans for Impact Level 6).

Rates
- ***TBD***

CS-ES-03: Department of Defense (DoD) Enterprise Portal Service (DEPS)

Overview

The DoD Enterprise Portal Service (DEPS) provides information sharing and collaboration capability based on Microsoft SharePoint based platform. It's available in shared and dedicated environments on NIPRNet and SIPRNet. Both environment types supply information management capabilities while protecting the organization's data. The offerings include document collaboration, content management, customizable search, social networking, business process automation, scalability, and COOP. The dedicated offering supplies the additional capability to host farm-level solutions in a customized and tailored package.

Rates
- ***DEPS Shared NIPR***
    - **RATE: $4.31** per user per month
- ***DEPS Implementation Shared NIPR***
    - **RATE: $26.06** per user
- ***DEPS Shared SIPR***
    - **RATE: $11.00** per user per month
- ***DEPS Implementation Shared SIPR***
    - **RATE: $49.91** per user

DEPS Dedicated rate:

- *Dedicated environments are engineered to the needs of each individual mission partner and pricing is based on the engineered solution.*

CS-ES-04: DoD Automated Time and Attendance Production System (ATAAPS)

Overview

This offering is a Human Resource Management System (HRMS) that provides information to downstream payroll processing by the Defense Civilian Payroll System (DCPS), entitlement systems, and in some cases enterprise resource planning (ERP) business systems. ATAAPS provides the ability to accurately record time and attendance while capturing labor hours by job order (task). ATAAPS creates a common platform for the DoD Agencies, Military Services, and Other Government Agencies (OGA) who use DCPS as their civilian payroll system of record. ATAAPS helps to ensure agencies can easily and effectively enter, validate, certify, audit, and transmit records to DCPS.

Rate
- **ATAAPS**
  - **RATE: $0.88** * per account per month

CS-ES-05: Global Content Delivery Service (GCDS)

Overview

Leverages commercial Internet technology to accelerate and secure DoD Web content and applications across the NIPRNet, SIPRNet, and CX-SOFTWAREA 24x7. GCDS' global platform of hundreds of specially-equipped servers helps the DODIN withstand the crush of daily requests for rich, dynamic, and interactive content, transactions, and applications. When delivering on these requests, GCDS detects and avoids DODIN related problem spots and vulnerabilities to ensure mission critical software downloads flawlessly, and applications perform reliably. The same platform also secures critical applications using its Web Application Firewall, allowing it to inspect web requests and detect application attacks before an organization's web server and data center is exposed to a possible threat. Furthermore, GCDS provides mission partners and security response teams with vital information that can be used to detect and block anomalous and potentially malicious attacks. Overall, GCDS provides the best user experience possible by not only increasing performance and availability anytime, anywhere for the warfighter, but also enhancing the security posture of an organization's data center to ensure mission partner's data is secured

24x7. GCDS is fully Type accredited with an Authority to Operate (ATO) on NIPRNet, SIPRNet and CX-SOFTWAREA.

GCDS is used for DoD Web Sites, Web-Based Applications and Video Streams
1. With end users on the NIPRNet, SIPRNet and / or CX-SOFTWAREA
2. Where speed and reliability are paramount in the criticality of the organization's missions
3. At the command level who need to get actionable information to the soldiers, sailors and airman quickly and efficiently
4. That must safeguard the value of users' content and enhance the security posture of the data and application
5. Who need to scale on-demand for peak loads, during both expected (e.g., promotion lists, commander's briefings) and unexpected events (e.g., Japan Tsunami)

GCDS Web Delivery

An HTTP / HTTPS content delivery managed service for NIPRNet and SIPRNet including 24x7 operational support, security accreditation and integration services. This service provides a DISN enterprise level service to accelerate delivery and improve the reliability of web applications. The managed service components include: End-User Mapping, Secure (HTTPS) Content Delivery, Advanced Cache Control, Compression Management, NOCC - Network Operations Command Center, Content Control Utility, Public Key Infrastructure, Robust Failover and a Customer Portal.

Rates
- ***GCDS URL Web Delivery***
    - **RATE: $894.10** per URL per month
- ***GCDS Implementation URL Web Delivery***
    - **RATE: $447.05** per URL

GCDS Storage

A storage repository managed service for NIPRNet and SIPRNet including operational support and security accreditation. This service provides a DISN enterprise level service to accelerate delivery and improve the reliability of network storage. Repository service capabilities include automatic content replication, scalability, high availability, dynamic mapping and flexible content management.

Rates
- ***GCDS Net Storage***

- **RATE: $11,749.07** per TB per month
- *GCDS Implementation Net Storage*
    - **RATE: $5,874.54** per URL

GCDS Web Application Firewall

A layer 7 firewall within the GCDS web delivery, storage and streaming services on NIPRNet and SIPRNet that prevents malicious attacks to include cross site scripting, SQL injection and others, and has the capability to detect the signature of the attack and block the attack if it were to occur across the GCDS services. WAF provides the capability to block users with certain identified IP blocks. It can counter DDOS attacks as well as handling flash crowds and load balancing globally.

Rates
- *GCDS Web Application Firewall*
    - **RATE: $119.40** per unit per month
- *GCDS Implementation Web Application Firewall*
    - **RATE: $59.70** per unit

CS-ES-06: FORGE.mil

Overview

Forge.mil is a family of enterprise services, consisting of SoftwareForge and ProjectForge, provided to support the DoD's technology community. The service provides for collaborative development and IT project management through the full application lifecycle. Forge.mil also enables the reuse of open source and DoD community source software. Forge.mil continues to add new capabilities to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. It is available as an open community service supporting anyone affiliated with the DoD, or as a private service, and is maintained on both the unclassified and classified networks. Forge.mil implements a set of tailorable net-centric processes and supporting infrastructure to:

- Promote early and continuous collaboration among all stakeholders
- Enable cross-program sharing of software, system components, and services
- Encourage modularity so that large programs to be developed, fielded, and operated as a set of independent components that can evolve at their own rate
- Allow organizations to test the security of applications quickly, accurately and affordably, without upfront investment of technology and resources

- Support agility and speed throughout the development life-cycle

Current Offerings
- SoftwareForge enables the collaborative development and distribution of open source software and DoD community source software.
- ProjectForge provides the same application life cycle management tools to DoD projects and programs as SoftwareForge, but for programs and / or projects that are not doing DoD community source development and / or need to restrict access to specific project members.

Rates
- ***Project Forge Small***
  - **RATE: $1,552.68** per user block per month
- ***Project Forge Medium***
  - **RATE: $3,881.70** per user block per month
- ***Project Forge Large***
  - **RATE: $15,526.78** per user block per month
- ***Software Forge***
  - **RATE: $620.23** per project per month

CS-ES-08: SKIWeb

Overview

Improves situational awareness for all Secure Internet Protocol Router Network (SIPRNet) users by organizing event-based information into a globally accessible, operationally relevant, and near real-time data store. Access enables Commanders, Action Officers, and other users to share data, plan strategies, develop Courses of Action (COA), assist in the decision making process, and make the necessary adjustments as situations develop.

- Provides a classified capability to meet mission requirements for organizing disparate data into an event-centric view to support global event situational awareness and management.
- Supports the event Lifecycle, where context and situational awareness of an event deepen over time, through individual knowledge and collaboration.
- Flattens the information chain to enable gathering of information from a wide range of user knowledge.
- Facilitates secure information sharing across the DoD, Intelligence Community, and select coalition partners.
- Provides access to real world events, improving the operational efficiency of intelligence gathering and sharing within diverse organizational communities.

Rate
- ***SKIWeb***
  - **RATE: $38.32** per user per month

CS-ES-09: Storage as a Service (STaaS)

Overview

Storage as a Service (STaaS) is a self-service, machine-to-machine object based storage solution capable of providing bulk storage for applications, backups, or system images available to all DoD agencies in the NIPR environment. STaaS is designed to offer high data availability and multi-site protection. The service allows mission partners to order storage on demand and scale as their data footprint grows at a low cost.

- No downtime during software upgrades, hardware refreshes and site failures
- Protects data from accidental deletion and corruption
- Cheaper than traditional block storage data backup services
- Compatible with Amazon S3 API
- Scaling storage capacity is simple, flexible and fast
- Supports very large data storage requirements (>100TB)
- Supports long term (7+ year) storage requirements
- Self-service ordering portal

Rate
- ***Storage as a Service (STaaS)***
  - **RATE: $0.30** per usable GB per month

**Section 6
Other Reimbursable Services**

CS-OR-01: Cyber Compliance

Overview

DISA Cyber Compliance Readiness is a mandatory service for all systems requiring financial statement audits as defined in the Financial Improvement and Audit Readiness (FIAR) list. This service will deliver independent audit opinions for DISA Information Technology (IT) General Controls, supporting evidence for the IT General Controls to support Mission Partner audit requirements. Cyber Compliance is only applied to production OEs (and not to dedicated COOP OEs.)

Rates
- ***Cyber Compliance IBM Mainframe***
    - **RATE: $2.62** per CPU Hour per month
- ***Cyber Compliance Open Systems***
    - **RATE: $362.50** per OE per month
- ***Cyber Compliance Unisys Mainframe***
    - **RATE: $0.24** per SUPS per month

CS-OR-05: Customer Management (CM) Charge

Overview

DISA assesses a CM charge to all recurring workload which recovers the costs necessary to provide mission partner support for engineering, project implementation, and recurring mission partner account management. The CM charge is not applied to DEE, DEPS, implementations, and some pass-thru reimbursable service offerings. A lower CM charge is applied to some Enterprise Services.

Rate
- ***Customer Management (CM) Charge***
    - **RATE: 4.87%**