Army Enterprise Service Desk (AESD) IV Performance Work Statement

The AESD Service Desk requires the following support:

Once a user's location or application being used is added to the contract, the Service desk support shall consist of the following services and support:

Service Desk Support for all Army I.T. user issues or concerns with I.T. operations or access to necessary applications. The AESD operator shall provide support 24 hours a day, 7 days a week, 365 days a year at a the AESD operator's proposed site and will include a continuity of operations (COOP) facility as back up operations for NIPR. The operator shall also support SIPR service desk 24 hours a day 7 days a week at a Government provided facility. The number of agents supporting the desk shall flex based upon call volume and all contract metrics shall be met.

See Attachment 0004 Minimum Guarantee Installations for locations and service desk coverage at time of initial award. See Attachment 0005 Federation membership for forecast of ticket volumes.

- The use of Information Technology Infrastructure Library (ITIL) Service Management model will be required. The ITIL model definitions for user support for incident handling are characterized as follows:

    - Tier 0 Self Service – Tier 0 is defined as self-help requiring no direct contact between an End User and a Customer Service Agent. The user is able to access a web-based portal to consult frequently asked questions, reference material, knowledge bases, or other information to resolve an incident. If the user is not able to resolve their issue through use of the various knowledge tools, the user is able to initiate a ticket, which describes the incident, problem, or service request and is sent to a support organization to triage the incident for resolution activities.

    - Tier 1 – The support organization that has the initial contact with the user and initiates tickets as required for issues. Tier 1 Agents are call center-based and provide non-dispatched basic problem assistance for issue resolution delivered via telephone, e-mail, web form, or other online communication channel. These agents make the computing environment less vulnerable by correcting flaws and implementing controls in the hardware or software installed within their operational systems. These agents may be required to have limited elevated privileges on local workstations to accomplish their tasks.

    - Tier 2 – The support organization that is responsible for further investigation and resolution of tickets unable to be resolved by Tier 1. This support organization is staffed with subject matter experts and more detailed reference materials. In the process of resolving incidents, this support organization may make substantial changes to ongoing operations in order to preclude future incidents of a similar nature from occurring as well as provide on-site solutions with dispatched touch labor.

- The AESD operator shall provide Software as a Service (SAAS) requirements for the software tool suite of integrated call management, service management, and workforce management systems. SAAS is defined as: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- The AESD Operator will make these managed SAAS capabilities available for Government use on NIPR. Within 6 months of contract award, the Contractor shall replace the Government's ticketing system supporting SIPR C4IM services with a SIPR ticketing/service management system instance supporting up to 2000 Government resolvers hosted on-premise at a designed Army site or in a RMF level 6 approved cloud-based hosting environment.

- The AESD operator shall comply with the Army Enterprise Service Management Framework (AESMF) as described in the DoD Enterprise Service Management Framework (DESMF) and ITIL. See attachments 0008 and 0009 to the RFP.

- The AESD Operator shall be required to have and maintain International Organization for Standardization 1428 (ISO)/International Electro technical Commission (IEC) 20000-1429 1:2011, Information Technology – Service Management.

- The AESD Operator shall be required to have and maintain a NIPR circuit at its commercial facilities. As such only Government Furnished computers and networking equipment is allowed on the NIPR/SIPR

- The AESD Operator shall provide Agent support at Government Provided Facilities for SIPR.

- The AESD Operator shall have successful Certification and Accreditation (C&A) of any systems supporting AESD (including commercially owned and operated systems managed by the Contractor and its subcontractors); obtaining a full Authority to Operate (ATO) before being granted operational status;

- The AESD Operator shall require that Contractor employees supporting AESD shall be citizens or legal residents of the United States. All Contractor personnel providing services and managed capabilities shall be considered Emergency Essential, regardless of assigned working location.

- The AESD operator shall ensure that at least 60% of the agents be facility-based (not remote agents) This requirement Excludes Contractor personnel working onsite at Government locations, at least 60% of the Contractor's remaining agents and support personnel shall work full time in person at the Contractor's primary or secondary sites

- The AESD Operator shall ensure that for the Sensor function, the normal functioning of the AESD produces information concerning timing, quantity, and impact of events and incidents which form the basis for an initial set of trend analysis reporting to ARCYBER ACOIC for operational use. Such information must be available generically and provided as part of analysis reports against Commander's Critical Information Requirements (CCIR) as published by ARCYBER.

- The AESD Operator shall ensure that Qualifications, training, and certification requirements of personnel are met as summarized in Attachment C although individual information assurance or Army policies that may change prior to or during the period of performance will have precedence over the Attachment C summary.

- The AESD Operator shall Maintain reserve resources necessary to support up to an additional 20% surge in projected daily demand without impact on established performance metrics

- The AESD Operator shall be responsible for entering and maintaining data within PEO EIS portal that contains all the Government's processes and knowledge articles, as well as within the EMASS system for accreditation.

- The AESD Operator shall comply with all applicable Federal, State and Local safety, health and environmental regulations, including the National Environmental Policy Act (NEPA). When proposed work under this contract is to occur on a military installation, the environmental consequences of all facility and mission work to be accomplished must be reviewed and approved by the Installation Environmental Office prior to execution of work. All permitting activities, e.g., Clean Water Act, Title 5 Air Permits and other required approvals must be obtained thru the Installation Environmental Office to ensure the contract performance is in full compliance with the commander and installation operating policies and permits.

-

- The AESD Operator shall be responsible for performing to all Army Information Assurance (IA) requirements. The Contractor and all of its subcontractors shall comply with IT security policy requirements, specifically those set forth in the Department of Defense Instructions (DODI) 8500.2, DODI 8520.2, DODI 8551.1, The Contractor and all of its subcontractors shall further comply with all applicable Federal IT security requirements including, but not limited to, the FISMA of 2002 and FedRAMP. The Contractor shall adhere to the following documentation or any revisions/updates thereof in the performance of all tasks:

- Army Regulation 25–1, "Army Information Technology" dated June 25, 2013
- Army Regulation 25–2, "Information Assurance" dated October 24, 2007; Rapid Action Revision (RAR), Issue Date: March 23, 2009
- Army Regulation 380–5, "Department of the Army Information Security Program" dated September 29, 2000
- Army Regulation 380–49, "Industrial Security Program" dated March 20, 2013
- Army Regulation 380–53 "Communications Security Monitoring" dated January 23, 2012
- Army Regulation 380–67, "Personnel Security Program" dated January 24, 2014
- Army Regulation 381-12, Threat Awareness and Reporting Program, October 4, 2010
- Army Regulation 500–3, "U.S. Army Continuity of Operations Program Policy and Planning" dated April 18, 2008
- Army Regulation 530–1, "Operations Security " dated September 26, 2014
- Army Regulation 700-142, Type Classification, Materiel Release, Fielding and Transfer dated June 2, 2015
- Army Regulation 735-5, Property Accountability Policies dated August 22, 2013
- Army Regulation 735-11-2, Reporting of Supply Discrepancies dated 6 August 2001
- CJCS Instruction 6510.01F, "Information Assurance (IA) and Computer Network Defense (CND)" dated 9 February 2011
- CJCS Memorandum 6510.01B, “Cyber Incident Handling Program,” December 18, 2014
- Computer Security Act of 1987 (Public Law No. 100-235 (H.R. 145)) dated January 8, 1988
- DCI Directive 6/3, “Protecting Sensitive Compartmented Information within Information Systems” dated June 5, 1999
- DCI Directive 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)” dated July 2, 1998
- DCI Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities” dated November 18, 2002
- Defense Acquisition Guidebook – Chapter 7, “Acquiring Information Technology” dated December 8, 2008
- Defense Information Systems Agency (DISA) IAVM Process Handbook, Ver. 3, dated February 2007
- Department of the Army Pamphlet 25–1–1, "Army Information Technology Implementation Instructions " dated September 26, 2014
- Department of the Army Pamphlet 25–1–2, "Information Technology Contingency Planning" dated June 6, 2012
- DFARS Subpart 204.73, “Safeguarding Covered Defense Information and Cyber Incident Reporting” (see also DFARS Subparts 202, 212, & 252) maintained at https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm
- DFARS Subpart 239.71, “Security and Privacy for Computer Systems” dated September 21, 2015

- DFARS 252.239-7001, ”Information Assurance Contractor Training and Certification” dated November 30, 2015
- DFARS Subpart 239.76, “Cloud Computing” (see also DFARS Subpart 252) maintained at https://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm
- DoD 5200.2-R, “Personnel Security Program” dated January 1987 (Administrative Reissuance Incorporating through Change 3, February 23, 1996)
- DoD 5400.11-R, “Department of Defense Privacy Program” dated May 14, 2007
- DoD 6025.18-R “DoD Health Information Privacy Regulation” dated January 24, 2003
- DoD CIO Memo "Certification and Accreditation Requirements for DoD Managed Enterprise Services Procurements" dated June 22, 2006
- DoD Information Assurance Vulnerability Alert (IAVA) memorandum dated December 30, 1999
- DoD Directive 3020.26, " Defense Continuity Programs (DCO)" dated January 9, 2009
- DoD Directive 5400.11, “DoD Privacy Program” dated October 29, 2014
- DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)" dated March 17, 2016
- DoD Directive 8140.01, “Cyberspace Workforce Management” dated August 11, 2015
- DoD Directive 8320.02, “Data Sharing in a Net-Centric Department of Defense” dated December 2, 2004 – Certified Current as of April 23, 2007
- DoD Directive 8140.01, “Cyberspace Workforce Management,” July 31, 2017
- DoD Directive 8500.01E, "Information Assurance” dated October 24, 2002; Certified Current as of April 23, 2007
- DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crises" dated November 6, 1990, Administrative Reissuance Incorporating Change 1, January 26, 1996
- DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)" December 30, 1997
- DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance” dated July 14, 2015
- DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology dated March 12, 2014
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System" dated July 9, 2004
- DoD Instruction 8910.01 “Information Collecting and Reporting” dated May 19, 2014
- DoD IPv6 Standard Profiles for IPv6 Capable Products Version 6.0 dated July 2011
- DoD Manual 5220.22-M "National Industrial Security Program Operating Manual (NISPOM)” dated February 28, 2006
- DoD Instruction 8570.01, Certifications Requirements, August 15, 2004

- DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program " dated 19 December, 2005 - Incorporating Change 4, dated November 10, 2015
- DoD Memorandum "Disposition of Unclassified DoD Computer Hard Drives" dated June 4, 2001
- E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. §101, H.R. 2458/S. 803) enacted on December 17, 2002, with an effective date for most provisions of April 17, 2002
- FAR 52.224-1 -- Privacy Act Notification (APR 1984)
- FAR 52.224-2 -- Privacy Act (APR 1984)
- Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules” dated May 25, 2001 and revised December 3, 2002
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) dated January 2008 (WH release on Comprehensive National Cybersecurity Initiative, March 2, 2010)
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "Revised Fact Sheet National Information Assurance Acquisition Policy" and associated "Frequently Asked Questions" dated January 2000, and revised July 2003
- NIST Special Publication 800-53 Revision 4, " Security and Privacy Controls for Federal Information Systems and Organizations" dated April 2013
- NIST Special Publication 800-145 maintained at https://csrc.nist.gov/publications/detail/sp/800-145/final
- NIST Special Publication 800-171, “Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations” maintained at https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- Office of Management and Budget (OMB) Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employee and Contractors, 3 February 2011
- OMB Circular A-130 (57 FR 18296) dated April 29, 1992 (Transmittal No. 4 dated November 28, 2000)
- OMB M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 25, 2007
- The National Security Act of 1947 (Pub. L, No. 235, 80 Cong., 61 Stat. 496, 50 U.S.C. Ch 15) dated July 26, 1947
- Section 3541 of title 44, United States Code, “Federal Information Security Management Act of 2002” (FISMA)Strategic Command Directive (SCD) 527-1, “Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures” dated 27 January 2006
- Public Law 107-347, 44 U.S.C. § 101; E-Government Act of 2002, Title III: Information Security (Federal Information Security Management Act of 2002 (FISMA)) dated December 17, 2002
- The Privacy Act of 1974, 5 U.S.C. § 552v (2015 Edition)

- Clinger Cohen Act of 1996, Title 40 (Pub L. 104-106, Division E) dated February 10, 1996
- DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crises" dated November 6, 1990, Administrative Reissuance Incorporating Change 1, January 26, 1996
- Memorandum of Agreement between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017 maintained at https://dcms.uscg.afpims.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6-/The-Office-of-Information-Management-CG-61/Interagency-Agreements/
- DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems" of June 6, 2012
- Federal Risk and Authorization Management Program (FedRAMP)
- Presidential Executive Order 13800 – "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017
- Department of Defense (DOD) Cloud Cyberspace Protection Guide of 16 October 2017 maintained at https://iasecontent.disa.mil/stigs/pdf/DOD_Cloud_Cyberspace_Protection_Guide-16_Oct_2017.pdf
- DoD Cloud Computing Security Requirements Guide, Version 1, Release 2, Mar 18, 2016 maintained at https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf
- Army Chief Information Officer (CIO)/G-6, "Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)," Aug 10 2015
- Army Chief Information Officer/G-6, Army Cloud Computing Strategy, March 2015
- Army Data Center Consolidation Plan (ADCCP) maintained at http://www.eis.army.mil/ec/ec-program-initiatives
- Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems (CNSS), March 27, 2014
- CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, April 06, 2015
- Creating Effective Cloud Computing Contracts for the Federal Government, February 12, 2012

Information Management

- The Department of Defense Architecture Framework (DoDAF) Version 2.0, 28 May 2009

Smart Cards

- Department of Defense Instruction (DoDI) 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals, January 23, 2014
- Army CAC/PKI Program Card Reader Specifications. 7 March 2007, https://chess.army.mil/ascp/commerce/scp/downloads/standardspolicy_files/2007_03_07_the_smart_card_update.pdf
- Smart Card Adoption and Implementation. 10 November 1999, http://www.cac.mil/assets/pdfs/DEPSECDEF_Policy.pdf
- DoD Directive 8190.3, August 31, 2002, Smart Card Technology , http://www.cac.mil/assets/pdfs/DoDD_81903.pdf

Section 508

- Section 508. http://www.section508.gov
- Section 508 – Electronic and Information Technology. 21 December 2000, http://www.usdoj.gov/crt/508/508law.pdf
- Desktop and Portable Computer (1194.26).

DoD and Army Documents

- Joint CONOPS Concept of Operations for Global Information Grid - Army, NETOPS CONOPS
- Defense Information Infrastructure Master Plan, Version 7.0
- Deputy Under Secretary of Defense (Logistics and Materiel Readiness) Logistics Enterprise Integration and Transformation http://www.acq.osd.mil/log/logistics_materiel_readiness/organizations/lsm/assetts/feb_02_information/ei_info/pdfs/Ent%20Integ%20and%20Transformation%20Dec%2001.pdf
- DISA Policy on Network Communications, http://www.fas.org/nuke/guide/usa/doctrine/dod/dodd-4660_3.htm

Records Management

- DoD Electronic Records Management Software Applications Design Criteria Standard. http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf

Other Regulatory and Commercial Requirements

- Distributed Management Task Force Desktop Management Interface (DMI) Version 2.0 http://www.dmtf.org/standards/dmi
- Security Requirements for Cryptographic Modules http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- Latest Windows 2000 and Windows NT Hardware Compatibility List ftp://ftp.microsoft.com/services/whql/hcl/win2000hcl.txt

References:

Department of Defense (DoD) Level Policy References

- Compliance with DoD Web Site Administration Policy, http://www.dodig.mil/Audit/reports/fy01/01-130.pdf, May 31, 2001
- Destruction of DoD Computer Hard Drives Prior to Disposal Memorandum by Deputy Secretary of Defense, http://iase.disa.mil/policy-guidance/destruction-of-dod-computer-hard-drives-prior-to-disposal-01-08-01.pdf, Jan 8, 2001
- Signed DoD Memorandum - Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf, Jul 03, 2007
- Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media Memo, http://iase.disa.mil/policy-guidance/faq_dar_encryption_policy_memo_18mar08_update-6_final.doc, Mar 19, 2008
- DoD IT Standards Registry (DISR) and DoD Acquisition Policy
- DoD Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement, http://iase.disa.mil/policy-guidance/dod-banner-9may2008-ocr.pdf, May 9, 2008
- DoD Telework Policy, http://www.dtic.mil/whs/directives/corres/pdf/103501p.pdf, Oct 21, 2010
- PEO EIS Policy-Telework Program Guidance maintained at https://peoeis.kc.army.mil/sites/G8/Pages/Policies.aspx
- PEO EIS Policies maintained at https://peoeis.kc.army.mil/sites/G8/Pages/Policies.aspx
- PD ES SCAR Policy maintained at https://peoeis.kc.army.mil/es/amd/SCAR/Pages/default.aspx
- DoD Web and Internet-based Capabilities (IbC) Policies , http://www.defenselink.mil/webmasters,
- DoD Web Site Administration Policies and Procedures (with amendments), http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html, Jan 11, 2002
- IA Section of the Draft Defense Acquisition Guidebook, http://iase.disa.mil/policy-guidance/ia-section-of-draft-defense-acquisition-guidebook.doc, Jul 9, 2004
- Open Source Software in the Department of Defense (DoD) Memorandum, http://cio-nii.defense.gov/sites/oss/2009OSS.pdf, May 28, 2003
- Web site OPSEC Discrepancies, http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DoD_webmasters.html, Jan 14, 2003
- Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) Certified Current April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf, May 5, 2004
- Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf, Jun 30, 2004

- Electronic Newspaper Policy, http://www.defenselink.mil/webmasters/policy/5120_4.html, May 29, 1996
- Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Directive Cancels DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))"
- DoD Directive 5215.1 Computer Security Evaluation Center, https://hsdl.org/?view&doc=1833&coll=limited, Oct 25, 1982
- Global Information Grid Overarching Policy, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf, Feb 10, 2009
- DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) Certified Current April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf, Apr 14, 2004
- Information Technology Portfolio Management, http://www.dtic.mil/whs/directives/corres/pdf/811501p.pdf, Oct 10, 2005
- Information Assurance (IA) Implementation. http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf, DoD Instruction 8500.2, Feb 6, 2003
- DoD Directive 8520.1, Protection of Sensitive Compartmented Information (SCI) June 13, 2011, http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf
- DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)" February 24, 2012
- DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations" Change 1, July 25, 2017
- DoD Directive O-8530.1 – Computer Network Defense (CND)
- DoD Instruction O-8530.2 – Support to Computer Network Defense (CND)
- DoD Directive 8530.1-M – Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process
- Ports, Protocols, and Services Management (PPSM), http://iase.disa.mil/ports/index.html, Aug 13, 2004
- DoD Cloud Computing Security Requirements Guide maintained at http://iase.disa.mil/cloud_security/Pages/index.aspx
- 32 CFR Part 236, "DoD Defense Industrial Base Cybersecurity Activities" maintained at https://www.gpo.gov/fdsys/pkg/CFR-2013-title32-vol2/pdf/CFR-2013-title32-vol2-part236.pdf
- 32 CFR 2002, "Controlled Unclassified Information" maintained at https://www.gpo.gov/fdsys/pkg/CFR-1998-title32-vol6/xml/CFR-1998-title32-vol6-part2002.xml
- FAR (48 CFR) Subpart 4.19, "Basic Safeguarding of Contractor Information Systems" (see also FAR Subparts 7, 12, & 52)
- DoD Instruction 5000.02, Enclosure 14, "Operation of the Defense Acquisition System", Aug 10, 2017

Department of the Army Policy References

- http://www.usapa.army.mil/pdffiles/r70_1.pdf, Army Acquisition Policy, Dec 31, 2003

Army Enterprise Standardization

- Army Enterprise Desktop Software Standardization (TECHCON 2004-005b). 5 Nov 2004.
- Memorandum Establishing Army MS ELA Software Inventory as Single Source for Obtaining MS Products. 04 February 2004
- Moratorium on Microsoft Products and Product Support Services. 19 June 2003. https://chess.army.mil/ascp/commerce/scp/downloads/contracts/aei-esc_ms/Moratorium_ltr.pdf

Networthiness Program

- Networthiness Certification Program 2 April 2003, (Requires AKO Login)
- Army Knowledge Management Guidance Memorandum Number 18 August 2001
- Army NETOPS CONOPS (version 1.0)
- SAIS-IOE-S, Memorandum, Subject: Networthiness Program (2 Apr 2003)
- Networthiness Certification Implementation Plan for Automated Information Systems, 5 May 04

DoD Information Technology Standards Registry

- DoD Information Technology Standards Registry Baseline Release 04-2.0. 22 December 2004
- DoD Information Technology Standards Registry (Note: Access to the DISR requires registration/login to the DISA DISR online website)
- Applicable mandatory standards in DISR shall be implemented by the Contractor

System Security

- CJCSM 3170.01B: Operation of the Joint Capabilities Integration and Development System. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf

The Contractor shall meet the following performance requirements specified as Service Level Agreements (SLAs) and Key Performance Indicators (KPIs).

ITEM	NAME	TYPE
1	First Contact Resolution	SLA
2	Average Speed to Answer	SLA
3	Abandonment Rate	SLA

4	Human Response Time -- to an Inquiry Submitted via Email or Web Form	KPI
5	Ticket Accuracy	SLA
6	AESD Customer Satisfaction	KPI
7	AESD CRM (Contractor-provided ticketing system) System Availability	SLA
8	Surge Support	KPI

The following tables describe these SLAs and KPIs in more detail.

1: ***First Contact Resolution***

1. SLA SUMMARY			
1A. TASK AREA	Sub-Task 1 - Army Enterprise Service Desk Operations	**1B. PERFORMANCE CATEGORY**	Responsiveness
1C. ITEM #	1	**1D. SLA NAME**	First Contact Resolution

2. SLA OVERVIEW	
2A. SLA DESCRIPTION	Measures the efficiency and timeliness of AESD operations as indicated by the proportion of inbound calls, emails and web tickets to the AESD, which are resolved on the First Contact.
2B. RATIONALE	Incentivizes staffing of AESD with qualified AESD personnel to ensure maximum customer satisfaction.
2C. PERFORMANCE PERIOD	This SLA is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the period of performance
3. SLA MEASUREMENT	
3A. MEASUREMENT INTERVAL	The Measurement Interval is one (1) week
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on Sunday of the week and ends at 24:00 on Saturday of the week. Zulu time is used for the 24 hour period of measurement.
3C. SOURCE OF MEASUREMENT DATA	The source of measurement data is weekly reports from Ticketing system utilized.
3D. METHOD OF MEASUREMENT	SLA attainment is measured by: 1. A customer contacts AESD via phone, email or webmail 2. The incident is resolved within the Service Desk 3. If resolved on the First Call, the Agent asks the customer whether the incident has been resolved 4. If the customer responds in the affirmative the Agent asks if the ticket can be resolved 5. If the customer responds in the affirmative, the Agent resolves the ticket In the Ticketing System 6. This incident is considered resolved on the First Contact

	7. If resolved on the First Contact (Web/e-mail), the Agent resolves the ticket and a message is sent to the customer that the ticket is resolved. If the customer does not respond or re-open the ticket, the ticket is considered resolved on first contact.
3E. TIMING OF MEASUREMENT	SLA attainment is calculated after the end of the Weekly Measurement Period.
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	1. After resolution of the ticket, the ticketing system will automatically send the customer an email confirming their ticket has been resolved 2. The ticket will include the ticket number and instructions to the customer on how to contact the Service Desk to re-open their ticket, if the incident is not resolved, or if the incident should re-occur before the ticket auto closes. 3. Warm transfers where the incident is resolved by Tier 1-2 are considered Resolved on the First Contact 4. Tickets escalated to Tier 1-2 or external resolver groups and addressed through call-back are Unresolved on the First Contact 5. Tickets that result in a callback by any Tier are consider Unresolved on the First Contact
3H. EXCEPTIONS	1. Tickets generated while during downtime of Ticketing System ticketing system due to a network outage or network performance degradation outside the control of AESD are excluded from the calculation 2. Contacts that occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: a. Ticketing System downtime approved by the Government (e.g., for scheduled maintenance) b. Ticketing System downtime due to events outside AESD control and approved as such by the Government c. Failure of Monitoring Tools
4. SLA CALCULATION	
4A. CALCULATION	(NUMERATOR) Number of Successful Instances during 24 hour Measurement Interval ÷ (DENOMINATOR) Total

	number of Instances opened during 24 hour Measurement Interval = (RESULT) Service Level (%) Attained
4B. INSTANCE	Contact to the AESD
4C. NUMERATOR	Number of tickets resolved on the First Contact during the Measurement Interval
4D. DENOMINATOR	Total number of Contacts during Weekly Measurement Interval
4E. SUCCESS CRITERIA	A successful Call instance is a ticket resolved on the First Contact, wherein the customer agrees that the issue has been resolved. For web/email tickets, a successful Contact instance is a ticket resolved on first contact, wherein the customer does not re-open the incident
4F. DEFINITIONS	**Total number of Contacts during Measurement Interval** - all Contacts received by the AESD during the Measurement Interval regardless of whether they are determined to be "resolvable" on the First Contact
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	1. AESD is responsible for SLA attainment at of Responsibility (AOR) plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	65% for all other user communities 10.0% for local NEC services user community
5C. TARGET SERVICE LEVEL OBJECTIVE TIMEFRAME	85% for all other user communities 15.0% for local NEC services user community
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR

6. SLA ADMINISTRATION	
6A. REPORTING FREQUENCY	1. Reporting to commence at AOR 2. Daily reporting of results from: a. Prior day, b. Prior week ending yesterday c. Prior month ending yesterday d. Prior quarter ending yesterday e. Prior year ending yesterday 3. Weekend and Holiday reporting on next business day

	4. Monthly reporting of SLA attainment and root cause of SLA failures at the Monthly PMR
6B. NOTES AND COMMENTS	None

2: Speed to Answer

1. SLA SUMMARY			
1A. TASK AREA	Task 1 – AESD Operations	**1B. PERFORMANCE CATEGORY**	Responsiveness
1C. ITEM #	2	**1D. SLA NAME**	Speed to Answer
2. SLA OVERVIEW			
2A. SLA DESCRIPTION	Measures the efficiency and timeliness of AESD operations as indicated by the proportion of inbound calls to AESD, which are answered by an Agent in less than the specified timeframe		
2B. RATIONALE	Incentivizes staffing of AESD with qualified AESD personnel to ensure maximum customer satisfaction.		
2C. PERFORMANCE PERIOD	This SLA is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Task Order period of performance		
3. SLA MEASUREMENT			
3A. MEASUREMENT INTERVAL	The Measurement Interval is weekly		
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on Sunday of the week and ends at 24:00 on Saturday of the week		
3C. SOURCE OF MEASUREMENT DATA	The source of measurement data is ACD used by AESD.		
3D. METHOD OF MEASUREMENT	SLA attainment is measured by: 1. Querying the ACD for call statistics 2. Determining how many calls were answered by an Agent in less than the Minimum Service Level Objective (“Successful Calls”) during the Measurement Interval ; and 3. Counting the total number of calls received during the Measurement Interval (“Total Calls”)		

3E. TIMING OF MEASUREMENT	SLA attainment is calculated after the end of the Measurement Period; the calculation of Speed to Answer begins at the time the caller selects an IVR option.
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	Calls abandoned within the minimum SLA objective goal are not counted None.
4. SLA CALCULATION	
4A. CALCULATION	(NUMERATOR) Number of Successful Instances during Measurement Interval ÷ (DENOMINATOR) Total number of Instances during Measurement Interval = (RESULT) Service Level (%) Attained
4B. INSTANCE	Call to AESD
4C. NUMERATOR	Number of successful Calls during Measurement Interval
4D. DENOMINATOR	Total number of Calls during Measurement Interval
4E. SUCCESS CRITERIA	A successful Call is one to AESD, which is answered by an Agent in the specified timeframe or less from the time the caller selects an option.
4F. DEFINITIONS	None
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	1. AESD is responsible for SLA attainment at AOR plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	85.0% in less than 90 seconds
5C. TARGET SERVICE LEVEL OBJECTIVE TIMEFRAME	90.0% in less than 90 seconds
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. SLA ADMINISTRATION	

6A. REPORTING FREQUENCY	1. Reporting to commence at AOR Daily reporting of results from: a. Prior day, b. Prior week ending yesterday c. Prior month ending yesterday d. Prior quarter ending yesterday e. Prior year ending yesterday 2. Weekend and Holiday reporting on next business day 3. Monthly reporting of SLA attainment and root cause of SLA failures at the Monthly PMR
6B. NOTES AND COMMENTS	None

3: ***Abandonment Rate***

1. SLA SUMMARY			
1A. TASK AREA	Task 1 – AESD Operations	**1B. PERFORMANCE CATEGORY**	Responsiveness
1C. ITEM #	3	**1D. SLA NAME**	Abandonment Rate
2. SLA OVERVIEW			
2A. SLA DESCRIPTION	Measures the efficiency and timeliness of AESD operations as indicated by the proportion of inbound calls to AESD in which the caller disconnects before speaking to an agent.		
2B. RATIONALE	Incentivizes staffing of AESD with qualified AESD personnel to ensure maximum customer satisfaction.		
2C. PERFORMANCE PERIOD	This SLA is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Task Order period of performance		

3. SLA MEASUREMENT	
3A. MEASUREMENT INTERVAL	The Measurement Interval is weekly
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on Sunday of the week and ends at 24:00 on Saturday of the week

3C. SOURCE OF MEASUREMENT DATA	The source of measurement data is ACD used by AESD.
3D. METHOD OF MEASUREMENT	SLA attainment is measured by: 1. Querying the ACD to determine how many calls were disconnected before the caller spoke to a live agent; 2. Counting the number of calls disconnected before the caller spoke to a live agent ("Abandoned Calls"); and 3. Counting the total number of calls received during the Measurement Interval ("Total Calls")
3E. TIMING OF MEASUREMENT	SLA attainment is calculated after the end of the Measurement Period.
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	1. Calls abandoned within the minimum SLA objective goal are not counted
4. SLA CALCULATION	
4A. CALCULATION	(NUMERATOR) Number of Unsuccessful Instances during Measurement Interval ÷ (DENOMINATOR) Total number of Instances during Measurement Interval = (RESULT) Service Level (%) Attained
4B. INSTANCE	Call to AESD
4C. NUMERATOR	Number of unsuccessful Calls during Measurement Interval
4D. DENOMINATOR	Total number of Calls during Measurement Interval
4E. SUCCESS CRITERIA	An Unsuccessful call is one, which is abandoned prior to an Agent picking up.
4F. DEFINITIONS	1. Abandoned Call – A call during which a caller selects an option from the Voice Response Unit and hangs up the call prior to the call being answered by a live Agent.
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	1. AESD is responsible for SLA attainment at AOR plus 30 calendar days

5B. MINIMUM SERVICE LEVEL OBJECTIVE	Less than 5.0%
5C. TARGET SERVICE LEVEL OBJECTIVE TIMEFRAME	Less than 3.0%
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. SLA ADMINISTRATION	
6A. REPORTING FREQUENCY	1. Reporting to commence at AOR 2. Daily reporting of results from: a. Prior day, b. Prior week ending yesterday c. Prior month ending yesterday d. Prior quarter ending yesterday e. Prior year ending yesterday 3. Weekend and Holiday reporting on next business day 4. Monthly reporting of SLA attainment and root cause of SLA failures at the Monthly PMR
6B. NOTES AND COMMENTS	None

4: ***Response Time to an Inquiry Submitted via Email or Web Form***

1. KPI SUMMARY			
1A. TASK AREA	Task 1 – AESD Operations	**1B. PERFORMANCE CATEGORY**	Responsiveness
1C. ITEM #	4	**1D. KPI NAME**	Human Response Time – to an Inquiry Submitted via Email or Web Form

2. KPI OVERVIEW	
2A. KPI DESCRIPTION	Measures proportion of AESD responses to Email or Web Form inquiries that are executed on a timely basis.
2B. RATIONALE	Incentivizes staffing of AESD with qualified AESD personnel to ensure maximum customer satisfaction.
2C. PERFORMANCE PERIOD	This KPI is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Task Order period of performance
3. KPI MEASUREMENT	
3A. MEASUREMENT INTERVAL	The Measurement Interval is weekly
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on Sunday of the week and ends at 24:00 on Saturday of the week
3C. SOURCE OF MEASUREMENT DATA	The source of measurement data is Ticketing System.
3D. METHOD OF MEASUREMENT	KPI attainment is measured by: 1. Querying the Ticketing System ticketing system to identify all tickets opened due to Email or Web Form inquiry 2. Counting number of tickets where the period between receipt of the Email or Web Form and the CSR's direct contact with the Email sender is less than the Minimum Service Level Objective ("Successful Responses") 3. Counting all Email or Web Form inquiries received over the Measurement Interval ("All Responses")
3E. TIMING OF MEASUREMENT	KPI attainment is calculated after the end of the Measurement Period.

3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	1. Ticketing System will execute a timestamp at the time of receipt of the Email or Web Form inquiry 2. Ticketing System will execute a timestamp at the time of the CSR contacting the End User by voice or email
3H. EXCEPTIONS	None
4. KPI CALCULATION	
4A. CALCULATION	(NUMERATOR) Number of Successful Instances during Measurement Interval ÷ (DENOMINATOR) Total number of Instances during Measurement Interval = (RESULT) Service Level (%) Attained
4B. INSTANCE	Responses to Email or Web Form inquiries
4C. NUMERATOR	Number of successful Responses to an Email or Web Form inquiries during Measurement Interval
4D. DENOMINATOR	Total number of Responses to an Email or Web Form inquiries during Measurement Interval
4E. SUCCESS CRITERIA	A successful Response to an Email or Web Form inquiry is one executed in less than the Service Level Objective
4F. DEFINITIONS	None

5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	1. AESD is responsible for SLA attainment at AOR plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	90.00% in less than six (6) hours
5C. TARGET SERVICE LEVEL OBJECTIVE TIMEFRAME	95.00% in less than six (6) hours
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR

6. KPI ADMINISTRATION	
6A. REPORTING FREQUENCY	1. Reporting to commence at AOR 2. Daily reporting of results from: a. Prior day, b. Prior week ending yesterday c. Prior month ending yesterday d. Prior quarter ending yesterday e. Prior year ending yesterday 3. Weekend and Holiday reporting on next business day 4. Monthly reporting of KPI attainment and root cause of SLA failures at the Monthly PMR
6B. NOTES AND COMMENTS	None

5: Ticket Accuracy

1. SLA SUMMARY			
1A. TASK AREA	**1**	**1B. Performance Category**	**Quality**
1C. ITEM #	**5**	**1D. SLA Name**	**Ticket Accuracy**
2. SLA OVERVIEW			
2A. SLA DESCRIPTION	Measures accuracy and completeness of AESD-generated ticket documentation as indicated by the number of errors in tickets.		
2B. RATIONALE	Supports improved root cause analysis in problem resolution		
2C. PERFORMANCE PERIOD	This SLA is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Contract period of performance		
3. SLA MEASUREMENT			
3A. MEASUREMENT INTERVAL	The Measurement Interval is one (1) month		
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on the first day of the month and ends at 24:00 on the last day of the month		

3C. SOURCE OF MEASUREMENT DATA	The source of measurement data is the Contractor-provided and GFE Ticketing Systems.
3D. METHOD OF MEASUREMENT	SLA attainment is measured by: 1) The Government COR or designee will randomly sample between 500-1000 tickets during the Measurement Period ("Total Sampled Tickets") 2) Each ticket is analyzed for Ticket errors; where two (2) or more ticket errors are found the ticket is defined as an "Inaccurate Sampled Ticket"
3E. TIMING OF MEASUREMENT	SLA attainment is calculated at the end of the Measurement Period
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	None
4. SLA CALCULATION	
4A. NUMERATOR	Accurate Sampled Tickets
DIVIDED BY	
4B. DENOMINATOR	Total Sampled Tickets
4C. DEFINITIONS	None
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	Notice to Proceed until AOR plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	90.0% for all tickets
5C. TARGET SERVICE LEVEL OBJECTIVE	95.0% for all tickets

5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. SLA ADMINISTRATION	
6A. REPORTING FREQUENCY	Monthly
6B. REPORTING COMMENCEMENT	Reporting to commence at AOR
6C. NOTES AND COMMENTS	None

6: AESD Customer Satisfaction

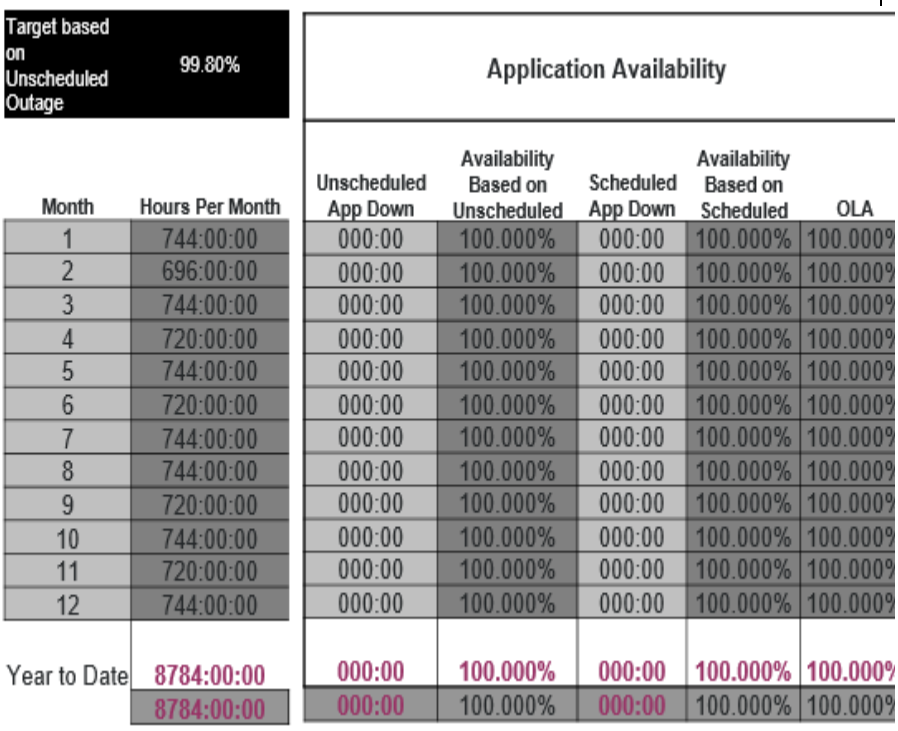
1. KPI SUMMARY			
1A. TASK AREA	1	**1B. Performance Category**	Quality
1C. ITEM #	6	**1D. KPI Name**	AESD Customer Satisfaction
2. KPI OVERVIEW			
2A. KPI DESCRIPTION	Measures user perception of AESD performance as indicated by the average evaluation given on post-call comment cards.		
2B. RATIONALE	Supports call handling process improvement and agent training concerns		
2C. PERFORMANCE PERIOD	This KPI is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Contract period of performance		
3. KPI MEASUREMENT			

3A. MEASUREMENT INTERVAL	The Measurement Interval is one (1) month
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on the first day of the month and ends at 24:00 on the last day of the month
3C. SOURCE OF MEASUREMENT DATA	The sources of measurement data are the Contractor-provided post-call survey capability, email surveys returned by customers, and the GFE ICE Customer Satisfaction Tracking System.
3D. METHOD OF MEASUREMENT	Post-call, this KPI is produced by accumulating the responses for each question by category and comparing the results to the objective values.
3E. TIMING OF MEASUREMENT	KPI attainment is calculated at the end of the Measurement Period
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	None
4. KPI CALCULATION	
4A. NUMERATOR	Responses categorized as Excellent or Good for each question
DIVIDED BY	
4B. DENOMINATOR	Total responses for each question
4C. DEFINITIONS	None
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	Notice to Proceed until AOR plus 30 calendar days

5B. MINIMUM SERVICE LEVEL OBJECTIVE	80.0% of responses for each question categorized as Excellent or Good for all AESD user communities
5C. TARGET SERVICE LEVEL OBJECTIVE	90.0% of responses for each question categorized as Excellent or Good for all AESD user communities
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. KPI ADMINISTRATION	
6A. REPORTING FREQUENCY	Monthly
6B. REPORTING COMMENCEMENT	Reporting to commence at AOR
6C. NOTES AND COMMENTS	None

7: AESD CRM System Availability

1. SLA SUMMARY			
1A. TASK AREA	1	**1B. Performance Category**	Responsiveness
1C. ITEM #	7	**1D. SLA Name**	AESD CRM System Availability
2. SLA OVERVIEW			
2A. SLA DESCRIPTION	System availability metric is 99.8% availability on a monthly basis and measures the availability of the AESD CRM system. Any outage caused due to the connection to the Army's NIPR network, or not the result of events or actions within the direct management and control of the Contractor are excluded when calculating the availability.		

2B. RATIONALE	Incentivizes provisioning and staffing of AESD CRM to ensure maximum customer satisfaction.
2C. PERFORMANCE PERIOD	This SLA is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Contract period of performance
3. SLA MEASUREMENT	
3A. MEASUREMENT INTERVAL	The Measurement Interval is one (1) month
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 on the first day of the month and ends at 24:00 on the last day of the month
3C. SOURCE OF MEASUREMENT DATA	The sources of measurement data is the onscreen monthly report from the technical AESD CRM platform indicating system availability.
3D. METHOD OF MEASUREMENT	Sample screen shot: 
3E. TIMING OF MEASUREMENT	SLA attainment is calculated at the end of the Measurement Period

3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	None
4. SLA CALCULATION	
4A. NUMERATOR	Uptime minutes in month = Total minutes in month – (Regular Scheduled Maintenance with an outage and approved change requests for an outage and Force Majure or disaster event) – total Priority 1 (Major impact to the US Army. Normal business operations cannot be conducted. Users are affected regionally, nationwide, or globally for an extended period of time and no Work Around is available) minutes in the month. Monthly Availability = Uptime minutes in the month (as defined above)
DIVIDED BY	
4B. DENOMINATOR	(Total Minutes in Month – (Regular Maintenance and approved change requests for an outage and Force Majeure or disaster event)).
4C. DEFINITIONS	None
5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	Notice to Proceed until AOR plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	99.8%
5C. TARGET SERVICE LEVEL OBJECTIVE	99.9%

5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. KPI ADMINISTRATION	
6A. REPORTING FREQUENCY	Monthly
6B. REPORTING COMMENCEMENT	Reporting to commence at AOR
6C. NOTES AND COMMENTS	None

8: Surge Support

1. KPI SUMMARY			
1A. TASK AREA	1	**1B. Performance Category**	Performance
1C. ITEM #	8	**1D. KPI Name**	Surge Support
2. KPI OVERVIEW			
2A. KPI DESCRIPTION	Measures Contractor compliance for having in place surge support to handle up to 20% over forecasted daily volume.		
2B. RATIONALE	Compares the Contractor's daily forecast with actuals and identifies instances where the Contractor did not have the 20% surge support in place. Daily calculation reduces masking of staffing gaps in monthly Average Speed to Answer and Abandonment Rate SLA reporting.		
2C. PERFORMANCE PERIOD	This KPI is in effect on a continuous basis 24 hours per day, 7 days per week without interruption throughout the Contract period of performance		

3. KPI MEASUREMENT	
3A. MEASUREMENT INTERVAL	The Measurement Interval is one (1) day
3B. MEASUREMENT PERIOD	The Measurement Period begins at 00:01 and ends at 24:00.
3C. SOURCE OF MEASUREMENT DATA	The sources of measurement data are the Contractor-provided daily forecast and the next day's scorecard.
3D. METHOD OF MEASUREMENT	On day 1, the Contractor will provide the forecast volume anticipated for day 2. On Day 3, the actuals for day 2 will be used to compute the Average Speed to Answer (ASA) and the Abandonment Rate (AR) for Day 2 and compared to the monthly SLA requirement for each. If the Contractor did not attain the ASA or AR SLA for Day 2, and if the actual Day 2 volume did not exceed 120% of forecast Day 2 volume, then the Contractor will have failed the Surge Support KPI for Day 2. Otherwise, the Surge Support KPI will be "NA" for Day 2.
3E. TIMING OF MEASUREMENT	The Surge Support KPI will be calculated every day of the month and the number of "Fails" will be reported in the monthly statistics and the PMR.
3F. METHOD OF GOVERNMENT SURVEILLANCE	Subject to random or planned audit by the Government or its third party designee
3G. ASSUMPTIONS/ CONDITIONS	None
3H. EXCEPTIONS	None
4. KPI CALCULATION	
4A. FAIL INDICATION	Marked as Fail for each day when (ASA or AR daily calculation against ASA or AR monthly SLA is not met) and Actual Volume does not exceed (1.20xForecast Volume).
4B. DEFINITIONS	None

5. PERFORMANCE OBJECTIVE	
5A. HOLD HARMLESS PERIOD	Notice to Proceed until AOR plus 30 calendar days
5B. MINIMUM SERVICE LEVEL OBJECTIVE	Not more than 5 fails per month
5C. TARGET SERVICE LEVEL OBJECTIVE	No fails per month
5D. SERVICE LEVEL OBJECTIVE TIMEFRAME	The Minimum and Target Service Level Objectives in cell 5B and 5C are effective as of AOR
6. KPI ADMINISTRATION	
6A. REPORTING FREQUENCY	Monthly
6B. REPORTING COMMENCEMENT	Reporting to commence at AOR
6C. NOTES AND COMMENTS	None

Deliverables

The Contractor shall provide the deliverables listed below in Attachment B. Individual task orders may have additional deliverables specified in each order. The Government does not waive its right to request additional deliverables under the Basic Contract, even if such requirements are not specifically listed herein. The contractor shall provide all deliverables to the contracting officer or as delegated to contract specialist or contracting officer representative (COR).

ATTACHMENT B – Deliverable List

The following deliverables are the responsibility of the Contractor:

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
1	Program Review Statistical Report	Summary presentation of AESD metrics, SLAs/KPIs attainment, and call volume analytics by category, priority, service, VIPs. Describes overall service performance activities for the previous month.	Monthly, no later than the 15th calendar day of the following month
2	Program Management Organization Chart	Identifies Key Personnel by name, position, contact information, supported organizations, and reporting relationships	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month
3	Standard Operating Procedures	Details all routine processes for operation and maintenance of AESD.	120 calendar days from award. After Government approval, updated monthly for any changes, no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
4	Security Management Plan	Describes IT Security approach and provides: •Contractor staff roles and responsibilities of the members of the Contractor IT Security Management organization •IT Security Threat Assessment process •IT Security Policy Statements •Vulnerability and incident identification process •An inventory list of IT Security Policy Statements •Approach for compliance with RMF •Handling of Security incident steps: Detection Identification Classification Recording Investigation Root Cause Analysis Remediation	60 calendar days from award. After Government approval, updated monthly for any changes, no later than the 15th calendar day of the following month
5	Integrated Master Schedule (IMS)	Depicts milestones, significant events, and internal/external dependencies for overall program, contract transition, onboarding, operations, and improvement projects	14 calendar days after award, updated every two weeks for Government review and approval

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
6	Quality Control Plan	Describes in detail how the Contractor ensures its employees deliver services and equipment that meet the performance standards.	60 calendar days from award. After Government approval, updated monthly for any changes, no later than the 15th calendar day of the following month
7	Score Cards	Daily, weekly and monthly reports in format approved by the Government for activity metrics providing: - Performance against all SLAs/KPIs - Call volume analytics by category/ class, priority, service and other attributes - all ticket volume by origination and type of ticket, number of open tickets, number of tickets assigned, unassigned tickets, time of acknowledgement, and mean time to restore (MTTR), VIP ticket handling - rolling summary of weekly, monthly, and year to date volume and performance metrics	Daily no later than 1200 EST of the following day, Weekly (Sunday through Saturday) no later than 1200 EST of the following Sunday, and Monthly no later than 1200 of the first day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
8	SLA/KPI Performance Management Remediation Plan	Provides root cause analysis for any SLA/KPI failure during the past month and: ·Describes remediation actions implemented or proposed improvements in response to SLA/KPI failures ·Identifies any availability issues outside of the Contractor's control that impacted SLA/KPI attainment	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month
9	SLA/KPI Attainment Report	Provides summary of previous month's SLA/KPI measurements, compares to previous months, analyzes Service Levels attained and recommends any improvements for all SLAs/KPIs in Government approved format. Also Identifies and tracks any barriers to SLA/KPI attainment or availability being remediated	Monthly, no later than the 15th calendar day of the following month
10	Risk Management Plan	Identifies, quantifies, and prioritizes risks against criteria for risk acceptance. Monitors risk occurrence and projects probability of risk occurrence. Provides mitigations for each identified risk Maintains all risks in Risk Register detailing impact levels, probability, impact, mitigation actions, risk owners, qualitative risk analysis, and risk response.	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
11	CCIR Report	Provide Commander Critical Information Reporting (CCIR) in Government-provided format	As directed in CCIR policy
12	GDA Assessment	Advise the Government of planned GDA implementation and any negatively impacted systems, processes, operational risk, potential performance measure failure, or contractual issue associated with the execution of GDA	As directed in the GDA issued
13	GDA After Action Report	Advise the Government of the GDA completion status, open issues pending resolution, and provide comparison of GDA assessment and actual implementation results	As directed in the GDA issued
14	GDA Tracker	Report date received, summary assessment, implementation status, after action status of all received GDAs	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
15	Transition Plan	Provide transition-in and transition-out activities. Transition-out includes: ·Coordination with Government representatives. ·Review, evaluation and transition of current support services. ·Transition of all current and historic data to new system. ·Transfer of all necessary business and/or technical documentation. -Transfer of all knowledge articles to the new system ·Transfer of hardware warranties and licenses (if applicable). ·Transfer of business rules, to include all versions, maintenance updates and patches (if applicable). Includes: ·Copies of all existing policies and procedures ·Extracts of existing data by the Contractor into Government-specified transfer formats ·Historical metrics and statistics	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
16	Services Availability Report	Reports the total time the Contractor and Government provided capabilities were available as a percentage of total time in the period.	Monthly, no later than the 15th calendar day of the following month
17	Forecast Report	Reports the utilization and forecasted requirements for any Government resources allocated to the Contractor and reports the Contractor projected resource requirements, staffing, and scheduling required to meet forecasted demand.	Daily Forecast in accordance with Surge Support KPI no later than 1200 EST; Weekly Report of detail from Work Force Management System no later than 0900 EST Monday of the following week.
18	COOP/DR Plan	Provided in accordance with AR 500-3 using primary and secondary sites at least 100 miles apart, circuit, facility, and operational redundancies, Identified RPO and RTO, and Program Level COOP/DR Plan	14 calendar days after award for Government Approval and updated monthly for any changes no later than the 15th calendar day of the following month
19	COOP/DR Exercise Results Report	Provided in accordance with Government approached approved COOP/ DR Plan.	Seven (7) business days after completion of the Exercise and monthly no later than the 15th of the month.
20	Service Asset and Configuration Management Implementation Plan	Describes the Contractor's approach to asset and configuration management of Contractor-provided managed capabilities.	Monthly no later than the 15th calendar day of the following month.

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
21	Inventory Report	Reports total inventory and changes during the quarter including any inaccurate inventory corrected.	Quarterly not later than the 15th of the first month following the end of the quarter.
22	Service Asset and Configuration Management Report	Report attributes, any linkage to physical assets, and relationships of configuration items necessary for IT service delivery	Monthly not later than the 15th of the first month following the end of the quarter.
23	Configuration Management Audit	Report Configuration Management activities	Monthly not later than the 15th of the first month following the end of the quarter.
24	Materiel Fielding Plan (MFP)	Outlines the specific activities, C4IM IT services, and infrastructure support IAW AESD MFP format in support of a service capability cutover.	As determined by the Notice to Onboard
25	Pre-site Survey	Identifies fielding information that is needed to inform the site survey process	Pre-site surveys issued three (3) weeks or more prior to the actual Site Survey
26	Site Specific Implementation Plan	Outlines the specific activities, C4IM IT services, infrastructure support, and meeting requirements in support of a service capability cutover. An SSIP is executed for each NEC that is on-boarded. Includes As-Is and To Be documentation.	Completed for each fielded installation

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
27	Pre-cutover Brief	Recaps on-boarding activities to gaining command, provides schedule for final cut- over with activities required to complete the on-boarding process, and provides the installation a “leave-behind” package.	No less than five (5) calendar days prior to Cutover.
28	After Action Review	Discusses the transition process between AESD and gaining command and captures discussion items (issues/concerns) for inclusion in Lessons Learned.	No later than seven calendar days after Cutover is complete
29	Lessons Learned Document	Provides analysis of the issues/concerns for the transition process between AESD and gaining command Strengths should discuss strategies and/or activities that led to success: • Weaknesses should discuss strategies for improvement • Post-fielding survey (gaining command responsibility) an important feeder	14 calendar days after Cut-over.

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
30	Installation or Organization “Leave Behind” Package	Includes: • In-brief • Site-specific implementation plan • Completed project plan • Data submitted by NEC • Tactics, Techniques & Procedures (TTPs) (as applicable) • Test and validation use cases and results • Documents installation points of contacts	Seven (7) calendar days after completion of fielding.
31	Scope Summary	Identifies requesting organization, service owner, service offering, users, volumes, anticipated timeline, dependencies, current service support structure (if any), and anticipated future service support structure in accordance with Government-provided template and examples.	As indicated in Notice To Proceed
32	Service Design Plan	Identifies changes and proposed service desk business process, agent training/skills, knowledge articles, technical changes, and other service support elements in accordance with the Government –provided examples.	As indicated in Notice To Proceed

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
33	Customer Service Agreement	Identifies ongoing point of contact and support processes for the service owner reference in accordance with the Government-provided examples.	As indicated in Notice To Proceed
34	Test Report	Describes testing activities and results on GFE and/or Contractor-provided managed capabilities.	As indicated in the Approved Change Request or Notice to Proceed
35	Change Evaluation Ad-Hoc Reports	Reports projected impact of change being evaluated using actuals	As indicated in the Notice to Proceed or Government Directed Action for the Change Request being evaluated
36	Change Evaluation Analysis	Documents "as is" business processes, assesses cost, risk, performance, and schedule impacts of potential changes in business processes and managed capabilities, develops detailed business process description documentation, and provides system integration analysis to identify changes for GFE and managed capability interoperability	As indicated in the Notice to Proceed or Government Directed Action for the Change Request being evaluated
37	CCIR After Action Report	Provides detailed CCIR impact assessment	As directed by CCIR policy
38	Service Request Report	Provide average timeline for fulfillment actions by service request type for all service requests	Monthly, no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
39	Problem Management Plan	The Problem Management Plan shall address, at a minimum: •Problem Recording and reporting formats, Management and Escalation processes •Processes to Analyze historical data to identify and eliminate potential incidents •Processes to Identify underlying causes of incidents to prevent recurrences and enable development of solutions to problems •Processes to Develop/ Suggest workarounds or other solutions to incidents •Processes to Suggest changes to eliminate known problems	14 calendar days after award and updated monthly for any changes no later than the 15th calendar day of the following month
40	Rolling Analytics Report	Summarizes business transaction volumes processed by each Contractor-provided Managed Capability by month for each month of the past year.	Monthly, no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
41	Ad Hoc Reports	Provides ad-hoc reporting, dashboard, and analytics to support Government queries or Government Directed Actions Reports and requested analytics for each Functional/Organization/ Service (User Community) Reporting by type, based on requirements for each new Functional/Organization/Service on- boarded.	Continued production of existing ad hocs as scheduled; additions made on case-by-case COR approval based on ad-hoc review during transition process; All others as indicated in the Notice to Proceed or Government Directed Action
42	Workforce Management Report	Reports changes by type and number made during the month to all resources maintained the Workforce Management System. Also compares total monthly scheduled and actual labor performed	Monthly, no later than the 15th calendar day of the following month

ID	Deliverable Name	Deliverable Description	Deliverable Due Date
43	AESD Federation COOP/DR Plan	The AESD Federation COOP/DR Plan shall include, at a minimum: Design redundancy directions, fall over plans, architectural considerations, and interoperability standards being applied to delivery of individual Task Order services and managed capabilities that enables AESD to operate as one desk with multiple locations. Development guidelines for Task Order COOP/DR Plans in order to provide comprehensive AESD Federation COOP/DR across supported AESD Federation Members for Government approved Recovery	60 calendar days after award and updated when new Task Orders are awarded or changes are made to the plan; updated 30 Calendar Days prior to Contract expiry

ATTACHMENT C – Job Description List

The Contractor shall verify United States citizenship for all personnel and the ability to speak, read, and write English fluently. In addition, AESD-K is required to have at minimum of 4 bilingual (English and Korean) agents on shift. Per the Information Assurance references, all Contractor personnel shall complete and maintain the following Army required Information Assurance (IA) certifications:

- DoD Cyber Awareness Challenge (Once per year)
- Derivative Classification (Once every 2 years)
- Derivative Training is 103.06 (initial training)
- Derivative Refresher Training is 109.16 (required every two years)
- Threat Awareness Reporting Program (TARP) (Once per year)
- Personal Identifiable Information (PII) v2.0 (Once per year)
- Personal Identifiable Information (PII) Memo (Once per year)

- Cyber Security Fundamentals (or the Information Assurance Fundamentals (IAF) (One time)
- Acceptable Use Policy (Once every 2 years)
- Privileged Level Access Agreement (PLAA) (One time) (Only for Agents with Elevated Privileges)

In addition to the above IA training/certification requirements, Contractor personnel requiring SIPR access will complete the following training/certification requirements:

- Introduction to Information Security (IF011.16 & IF011.06) (One time)
- Operation Security (OPSEC) Awareness for Military Members, DoD Employees and Contractors Course (GS130.16) (Once per Year)
- Information Security Program (Once per year)
- Security Classification Guidance (IF101.16 & IF101.06) (One time)
- Original Classification (IF102.16 & IF102.06) (One time)
- Marking Classified Information (IF105.16 & IF105.06) (One time)
- Unauthorized Disclosures of Classified Information (IF130.06 & IF130.16) (One time)104.06
- Anti-Terrorism Level 1 (Once a year)
- Information Security Program Training (once a year)

The Contractor shall be responsible for training, retraining if changes occur, and maintaining adequate numbers of trained agents in Army terminology, AESD operations, and supported services knowledge throughout the period of performance.

The following are job descriptions and skills requirements for Contractor positions that shall be used for standardized workflow planning, pricing, and execution:

Tier 1-1 Agent

The Tier 1-1 Agent is the first person an Army End User will speak with; therefore, this Agent must have superior customer service skills, possess a high technical aptitude, and be familiar with Army vernacular. The 1-1 Agent is the first POC for Army End Users, regardless of the communication channel, e.g., web submissions, phone, email, chat. To limit downtime to Army End Users, the 1-1 Agent must be able to elevate rights within the DoD networks. All Tier 1-1 Agents shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- CompTIA A+, N+, S+ continuing education (CE) or equivalent certification (according to IA requirements outlined in DoD 8570) (only one cert is required)
- Windows 10, or current version of Windows OS, course certification
- Strong customer service skills and technical aptitude

The Tier 1-1 Agent:

- Responds to and diagnoses problems through discussion with users.
- Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps.
- Supervises operation of help desk and serves as focal point for customer concerns.
- Provides support to end users on a variety of issues.
- Identifies, researches, and resolves technical problems.
- Responds to telephone calls, email and personnel requests for technical support.
- Documents, tracks, and monitors the problem to ensure a timely resolution.
- Provides second-tier support to end users for either PC, server, or mainframe applications or hardware.
- Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem.
- Simulates or recreates user problems to resolve operating difficulties.
- Recommends systems modifications to reduce user problems.

Tier 1-2 Agent

Tier 1-2 Agents will be responsible for resolving more complex issues than Tier 1-1 Agents. They will have access that Tier 1-1 Agents will not. They may be referred to as Level 2 (L2) Agents. Although an L2 Agent must have all the same qualifications as a Tier 1-1 Agent, L2s must also have the ability to coach Tier 1-1 Agents through difficult calls and complex technical issues. L2 Agents may be called on to interact with NEC personnel to relay outages or VIP tickets and provide surge support during periods of call spikes and outages. All Tier 1-2 Agents shall have at least the following

qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- CompTIA A+, N+, S+ CE or equivalent certification (according to IA requirements outlined in DoD 8570) (only one cert is required)
- Windows 10, or current version of Windows OS MCP certification
- ITIL V3 Foundations certification
- Strong customer service skills and technical aptitude

Tier 2 Agent

Tier 2 agents provide local touch labor. All Tier 2 Agents shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- CompTIA A+, N+, S+ CE or equivalent certification (according to IA requirements outlined in DoD 8570) (only one cert is required)
- Windows 10, or current version of Windows OS MCP certification
- ITIL V3 Foundations certification
- Strong customer service skills and technical aptitude

Program Manager (PM) (Key Position)

The Program Manager is defined as having responsibility for oversight of operational planning, establishment, execution, and evaluation of a multifaceted program/project typically consisting of a set of closely related sub-programs or associated activities. The PM should have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Helpdesk Institute Support Center Director Training
- ITIL Foundations & ITIL Operational Support and Analysis Training
- Secret Clearance

The PM:

- Oversees fiscal, operational, administrative, and human resources management of the program
- Serves as principal point of representation and liaison with external constituencies on operational matters

- Provides day-to-day technical/professional guidance and leadership as appropriate to PL EC, ARCYBER and CIO/G-6.
- The following experience is highly desirable, but not mandatory:
    - Demonstrated excellence and over 15 years planning, directing, and managing large scale IT operations and projects
    - Demonstrated successful management and supervision of employees of various labor categories and skills in efforts similar in size and scope
    - Knowledge of industry accepted standards and best practices related to IT management and development
    - Demonstrated experience in a DoD IT environment and an understanding of DoD culture and standards
    - Experience managing performance-based contract Task Orders and knowledge of Federal Acquisition Regulations (FAR)
    - Demonstrated ability for oral and written communication with the highest levels of management
    - Project Management Professional (PMP) certification
    - Knowledge of industry accepted standards and best practices related to Information Management operations, and Information Technology Service Management (ITSM) best practices.

Operations Manager (Key Position)

The Operations Manager is responsible for service desk operations and acts as the contractor liaison between the Government PM/COR and the Contractor's service desk workforce. Provide oversight of all locations, including CONUS and OCONUS. This individual will confirm that day-to-day activities are running efficiently and properly. The Operations Manager shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- ITIL Operational Support and Analysis certification
- Help Desk Institute Support Center Director certification
- CompTIA Security+ CE certification or equivalent
- Strong customer service skills and technical aptitude
- Have An understanding of DoD culture and standards

The Operations Manager shall:

- Ensure timely processes through which incidents and problems are managed. Includes problem recognition, research, isolation, resolution and follow-up steps.
- Optimize operations and processes to resolve less complex problems immediately, while more complex problems are escalated to next level support or supervisor
- Provide guidance/training for less experienced personnel
- Have at least 4 years overall IT Service Desk management or IT Service Desk operations experience
- Have at least 1 year of experience planning, directing, and managing service support operations in an organization similar in size to AESD
- Have knowledge of industry accepted standards and best practices related to Information Management operations, and with ITSM best practices

Technical Capability Manager (Key Position)

The Technical Capability Manager is responsible for operational planning, implementation, and operation of technical capabilities provided by the Contractor for service desk use such as the call management, workforce management, and ticketing systems. The Technical Capability Manager shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- ITIL Operational Support and Analysis certification
- CompTIA Security+ CE certification or equivalent
- Certified Information Systems Security Professional (CISSP) certification
- Familiarity with AR25-1 and AR25-2
- Experience with AESS/HBSS, SCCM, NESSUS ACAS, and POA&M submission
- Have An understanding of DoD culture and standards

The Technical Capability Manager shall:

- Develop and maintain compliance to the overall technical architecture that integrates the managed capabilities being provided to the Government
- Ensure timely processes through which incidents and problems are managed. Includes problem recognition, research, isolation, resolution and follow-up steps.
- Optimize operations and processes supporting managed capabilities
- Provide guidance/training for less experienced personnel
- Have at least 4 years overall DoD IT environment and RMF experience
- Have at least 4 years of IT Service Desk management or IT Service Desk operations experience

- Have at least 1 year of experience in planning, directing, and managing large scale IT operations in an organization similar in size to AESD
- Have knowledge of industry accepted standards and best practices related to Information Management operations, and with ITSM best practices

Change Manager (Key Position)

The Change Manager is responsible for planning and execution of assigned projects supporting change evaluation, contract transition, convergence, onboarding, and/or improvements. Provides a single point of contact for the status of those projects. The Change Manager shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- ITIL Operational Support and Analysis certification
- CompTIA Security+ CE certification or equivalent
- Have An understanding of DoD culture and standards

The Change Manager shall:

- Meet transition, on-boarding, and improvement project schedule goals
- Supervise activities of multidisciplinary teams supporting transition, on-boarding, and improvements
- Serve as primary Point of Contact for Government requirements staff
- Take projects from original concept through final implementation
- Interface with all areas affected by the project including end users, computer services, and client services
- Define project scope and objectives
- Develop detailed work plans, schedules, project estimates, resource plans, and status reports
- Conduct project meetings and is responsible for project tracking and analysis
- Ensure adherence to quality standards and reviews project deliverables
- Provide technical and analytical guidance to project team
- Recommend and takes action to direct the analysis and solutions of problems
- Have at least 4 years of IT Service Desk management or IT Service Desk operations experience
- Have at least 1 year of experience in planning, directing, and managing large scale transitions for an organization similar in size to AESD

- Have knowledge of industry accepted standards and best practices related to Information Management operations, and with ITSM best practices
- Optionally be Project Management Professional (PMP) Project Manager Certified
- Optionally have Help Desk Institute Support Center Manager Training

Project Manager (T&M Position)

Project Managers are responsible for managing a team conducting onboarding, improvement, GDA, or convergence activities. The Project Manager will transition services and commands to AESD and eliminate the replication of work that exists, with multiple entities each hosting their own Tier 0 and Tier 1 support to Army End Users. The Project Manager shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- ITIL Operational Support and Analysis certification
- ITIL Release, Control and Validation certification
- More than 8 years of experience managing large, complex projects
- An understanding of DoD culture and standards

The Project Manager:

- Leads team on large projects or significant segment of large complex projects.
- Analyzes new and complex project related problems and creates innovative solutions involving finance, scheduling, technology, methodology, tools, and solution components.
- Provides applications systems analysis and programming activities for a Government site, facility or multiple locations.
- Prepares long and short-range plans for application selection, systems development, systems maintenance, and production activities and for necessary support resources.
- Oversees all aspects of projects.
- Optionally be Project Management Professional (PMP) Project Manager Certified

Systems Analyst (T&M Position)

The System Analyst is responsible for leading the change evaluation process, reviewing and documenting current processes, and analyzing all aspects of processes and process interfaces in order to develop and improve processes and performance. The Systems Analyst will assess all major changes and verify that those changes are

integrated horizontally and vertically throughout the Army. In addition to the specific skills listed below, the Systems Analyst shall have experience in managing Department of the Army level enterprise information technology service programs like email, service desk operations, and collaboration services, throughout the service life cycle. The Systems Analyst shall have at a minimum the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL Operational Support and Analysis certification
- ITIL V3 Foundation certification
- CompTIA Security+ Certifications
- More than 3 years of experience on service department level staffs (e.g. Department of the Army Staff, CIO/G-6)
- More than 5 years of experience Division or Brigade Staff
- More than 5 years of experience managing large, complex projects
- An understanding of DoD processes, culture, and standards

The Systems Analyst:

- Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements.
- Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications.
- Provides consultation on complex projects and is considered to be the top level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.

Onboarding Team Member (T&M Position)

The Onboarding Team Member assists in the analysis of services and service support being onboarded to AESD. The Onboarding Team Member shall have at a minimum the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- Have an understanding of DoD culture and standards
- Have Organizational Change Management experience

- 3-5 years of progressive business experience and call center operations experience, including project management

The Onboarding Team Member:

- Responds to and diagnoses problems through discussion with users.
- Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps.
- Identifies, researches, and resolves technical problems.
- Documents, tracks, and monitors the problem to ensure a timely resolution.
- Interact with network services, software systems engineering, and/or applications development to identify and implement support processes
- Simulates or recreates user problems to resolve operating difficulties.
- Recommends systems modifications to reduce user problems.
- Documents “as is” and “to be” business processes.

Reporting Analyst (T&M Position)

The Reporting Analyst verifies that metrics and other data being reported are accurate and assists in the development of new queries to support onboarding, convergence, change evaluation, and service support improvements. The Reporting Analyst performs root cause analysis, technical troubleshooting, and problem resolution to find the root cause of assigned problems. The Reporting Analysis shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL Operational Support and Analysis certification
- ITIL V3 Foundation certification
- CompTIA Security + CE
- An understanding of DoD IT policy and standards

The Reporting Analyst:

- Serves as subject matter expert on AESD processes, service catalog, and underlying configuration data model used to support reporting.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.

- Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

System Administrator (T&M Position)

To support the government furnished equipment utilized by the mission partner, System Administrators are required in each site where equipment exists. System Administrators will support the day-to-day maintenance and inventory of the equipment and perform patch management. System Administrators shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL Operational Support and Analysis certification
- ITIL V3 Foundation certification
- AESS certification
- CompTIA Security + CE
- Microsoft MCP in Windows 10 or current Windows OS
- An understanding of DoD culture and standards

The System Administrator:

- Provides technical guidance for directing and monitoring information systems operations.
- Designs, builds, and implements network systems.
- Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity planning solutions.
- Monitors and responds to complex technical control facility hardware and software problems. Monitors and responds to hardware, software, and network problems.
- Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance.
- Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems.
- Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications.

- Plans large-scale systems projects through vendor comparison and cost studies.
- Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment.
- Provides quality assurance review and the evaluation of new and existing software products.
- Provides assistance and oversight for all information systems operations activities, including computer and telecommunications/communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations.
- Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals).
- Provides input to policy level discussions regarding standards and budget constraints.
- Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network and system performance.
- Troubleshoots network systems when necessary and makes changes or improvements to the network using established change management processes**.**

Information Assurance Specialist (T&M Position)

The Information Assurance (IA) Specialist assesses, documents, and assists in the verification that the Contractor's managed capabilities remain complaint and interface with the IA personnel throughout ARCYBER, NETCOM, PL EC, and other organizations as required over the lifetime of the contract. The IA Specialist shall have at least the following qualifications, in addition to those required to be DoD 8570.01-M and 8140.01 compliant:

- Secret Clearance
- ITIL V3 Foundations certification
- ITIL Operational Support and Analysis certification
- CompTIA Security+ CE certification or equivalent
- Certified Information Systems Security Professional (CISSP) certification
- Familiarity with AR25-1 and AR25-2
- Experience with AESS/HBSS, SCCM, NESSUS ACAS, and POA&M submission
- Have an understanding of DoD culture and standards

The IA Specialist:

- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Performs analysis, design, and development of security features for system architectures.
- Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers.
- Designs, develops, engineers, and implements solutions that meet security requirements.
- Provides integration and implementation of the computer system security solution.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.
- Ensures that all information systems are functional and secure.