

PERFORMANCE WORK STATEMENT – REVISION 1
INFORMATION TECHNOLOGY SERVICES AND SUPPORT
HAWTHORNE ARMY DEPOT
27 MAY 2010

1. Contractor Personnel:

Contractor personnel requiring access to a Department of Defense (DoD) Automated Information System (AIS) shall be classified with an Automated Data Processing (ADP) Position Sensitivity and may require additional security investigation(s) and/or training prior to being granted access to the AIS. Three categories (ADP I, II, and III) have been established for designating computer and computer-related positions. Specific criteria for assigning these categories are outlined in AR 380-67, Appendix K. The phrase “Automated Data Processing (ADP)” has changed to “Information Technology (IT)” and referred to as IT I, II, and III throughout AR 25-2.

- 1.1.** The Contractor shall submit additional security investigation requests for personnel meeting ADP I, II, or III criteria within the timelines as required by AR 25-2, paragraph 4-14.
- 1.2.** All contractor personnel who require access to a government Information Systems (IS) shall successfully complete the DoD Information Assurance (IA) Awareness training (approximately one hour long) prior to being granted access to the IS and annually thereafter. To successfully pass this training, students must receive 70% or greater on the exam and provide the certificate of completion to the HWAD Information Assurance Manager (IAM) or alternate designated government personnel as proof.
- 1.3.** Contractor personnel who require access to government Information Systems (IS) shall sign the command’s Acceptable Use Policy (AUP) prior to being granted access to the IS. Contractor personnel shall review and re-sign the AUP annually or as required due to revision.
- 1.4.** A HWAD ACO government staff member will sponsor and assist in establishing an AKO account for each contractor who requires access to a Government IS. The government Contractor Verification System (CVS) Trusted Agent (TA) will initiate and approve CVS applications for the contractor to obtain their CAC Cards.
- 1.5.** The contractor shall be responsible for completion and submission of the automated DD Form 1172-2 in CVS.
- 1.6.** Contractor personnel who require access to DoD AIS shall obtain a Common Access Card (CAC). The contractor shall incur all expenses related to CAC issuance for contractor personnel, including but not limited to travel costs to the Naval Air Station (NAS) Fallon, NV CAC issuance facility for each contractor personnel requiring a CAC, smart card readers, and software. CACs will be issued for a period of three years, or the individual’s term of service, employment, or association with the DoD, whichever is earlier. The CAC is required for access/authentication to the DoD/Army network and to

most DoD/Army restricted web sites and applications.

- 1.7. Contractor personnel who require elevated privileged access to a government IS, as defined in the IA BBP Training and Certification, Version 3.0, paragraph 16.a., shall sign the command Privileged-Level Access Agreement (PAA) AUP, Non-Disclosure Agreement (NDA), and complete required training and/or certifications as outlined in the IA BBP Paragraph 7. The scope of this contract requires at a minimum one System Administrator (SA) trained and certified at Information Assurance Technical (IAT) Level II as outlined in the IA BBP, Table1: DoD Approved Baseline Certifications.

2. Local Area Network (LAN) Services and Support

- 2.1. The Contractor shall facilitate, manage, and operate the HWAD NIPRNET LAN to support the HWAD ACO staff (up to 41 users) for services that include, but are not limited to, the administration of: Microsoft (MS) Active Directory (AD), MS Exchange E-mail, File and Print services, and Blackberry Enterprise Server (BES). The contractor shall utilize commercial best business practices (e.g., Information Technology Infrastructure Library (ITIL), IT Service Management (ITSM), and ISO/IEC 20000 standards, concepts, and policies) in the performance of these duties.
- 2.2. The Contractor shall adhere to all current and future DoD/Army regulations and standards pertaining to the operation and sustainment of the HWAD LAN to maintain availability to the NIPRNET and LAN services. These are normally increased security settings and policies over and above commercial best business practices for the purpose of enhancing security of the government IS. These additional security enhancements are usually issued in the form of Communications Task Orders (CTOs) and will be provided to the contractor by the HWAD IAM. The contractor shall implement the CTOs within the given suspense dates.
- 2.3. The Army CONUS-Theater Network Operations and Security Center (C-TNOSC) remotely administers the Army Top Level Architecture (TLA) network security stack (router, firewall, Intrusion Detection System, etc...). The Contractor shall support C-TNOSC with visual and/or hands-on support when required. Physical repair or replacement of parts is not included in this contract.
- 2.4. The Contractor shall provide notification to the HWAD ACO staff of planned or unplanned system maintenance, downtime, or degradation.
- 2.5. The contractor shall obtain approval from the HWAD IAM prior to connecting or installing non-DOD/Army issued IT hardware or software to the HWAD NIPRNET LAN. Installing non-DOD/Army issued hardware or software is prohibited without approval from the organizational Designated Approval Authority (DAA) in accordance with AR 25-1, paragraph 6-1.i.

3. Desktop Services and Support

The Contractor shall provide installation and maintenance of government purchased hardware and software on government purchased computer workstations. The baseline operating system (OS) and software installation will be in accordance with the Army Golden Master (AGM) program. A list of the current AGM baseline software is provided in Ref 8.10.

- 3.1. The Contractor shall install and maintain the baseline operating system (OS) and software on the HWAD staff government purchased workstations in accordance with the Army Golden Master (AGM) program. AGM updates are to be installed within 6 months of release.
- 3.2. Install additional government procured software as required. Installation of additional software will be accomplished only when directed and approved by the HWAD IAM or the designated alternate.
- 3.3. Install additional government procured peripheral IT hardware. Installation of additional hardware will be accomplished only when directed and approved by the HWAD IAM or the designated alternate.
- 3.4. The Contractor shall provide Tier I and Tier II support to resolve hardware, software, and IT issues for the HWAD ACO staff. Tier I includes first response helpdesk support. Tier II includes support to the Helpdesk or liaison with the C-TNOSC to resolve IT issues when necessary. The government will be responsible for procurement of replacement and repair parts for hardware and software requirements for the HWAD ACO staff.
- 3.5. The Contractor shall assist the HWAD ACO staff in maintaining a current inventory of software installed on the HWAD ACO staff workstations to support software license verification in accordance with AR 25-2, paragraph f.(11).
 - 3.5.1. Perform annual inventory certification. Initial inventory to be conducted within 60 days of contract commencement.
 - 3.5.2. Provide software inventory list to the HWAD staff personnel within 5 working days of request when required outside the annual reporting interval.

4. Information Assurance (IA) Services and Support

- 4.1. The Contractor shall, in coordination with the HWAD Information Assurance Manager (IAM), prepare and implement an Information Assurance Program that satisfies the requirements of AR 25-2, paragraph 2-30.
- 4.2. The Contractor shall install and operate Information System (IS) protective devices and software as required by the Department of the Army (e.g. operate firewalls, Intrusion Detection Systems, Antivirus software, etc...)
- 4.3. The Contractor shall inform and assist the installation HWAD IAM with reports of Information System Incident and Intrusion Reporting required by AR 25-2 Chapter 4,

Section VIII and any additional reporting requirements required by Army Computer Emergency Response Team (ACERT) messages. The government will provide the contractor with a current contact list for reporting IA incidents.

- 4.4. The Contractor shall ensure software updates, vendor patches (service packs, service releases), and Information Assurance Vulnerability Alerts (IAVAs), etc. are applied to all appropriate devices (computer workstations, servers, printers, routers switches, etc...) connected to the HWAD LAN and Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) prior to the suspense date/time imposed by the DoD, Army, HQ JMC, or HWAD ACO.
- 4.5. When required the Contractor shall provide compliancy reports of installed updates to the HWAD IAM prior to the suspense date time imposed by the DoD, Army, HQ JMC, or HWAD ACO.
- 4.6. The Contractor shall assist the HWAD IAM with the certification and accreditation of IS and networks which processes or transmits Army information, as required by Chapter 5 of AR 25-2. The HWAD IAM will be responsible for reporting to the Designated Approval Authority (DAA) .

5. Telephone and Facsimile Services and Support

- 5.1. The Contractor shall operate, maintain, and upgrade telephone switches, remote switches, nodes, and PBXs as required to support the HWAD ACO staff. Dial tone shall provide access to the Public Switched Telephone Network (PSTN), Federal Telecommunications System (FTS), and Defense Switched Network (DSN). The government will fund the cost for FTS and DSN circuits.
- 5.2. The Contractor shall provide dial tone to each HWAD ACO employee desktop and additional devices (e.g. facsimile). Any additional requirements will be directed and approved by the HWAD IAM or the designated alternate. The government will be responsible for procurement, replacement, and repair parts for their telephone equipment.
- 5.3. The Contractor shall provide each HWAD ACO employee with voice messaging transmission, reception, and message storage capability 24 hours per day except during maintenance downtime.
- 5.4. The Contractor shall provide telephone diagnostic and troubleshooting service for the HWAD ACO staff during normal working hours.

6. Video Teleconference / Cable TV Services and Support

- 6.1. The contractor shall maintain government furnished VTC Studio to include limited cable TV broadcasts to television monitors placed throughout the installation.

- 6.2. The contractor shall provide local touch labor (setup, troubleshooting, repairing, etc.) The Contractor shall respond within 1 hour after a trouble call is made. The VTC Studio shall be operational 98% of the time.

7. Mailroom Operations:

In accordance with AR 25-51, a single Official Mail Distribution Center (OMDC) will be established on the installation to receive process, dispatch and deliver incoming and outgoing official mail distribution. The contractor shall operate the installation OMDC and provide sorting and distribution of official USPS mail in accordance with this PWS and all regulations/policies/directives referenced in this PWS. The contractor shall deliver official mail to the administrative office of each organization on the installation that is authorized official mail services. Internal distribution of official mail and distribution within an organization is the responsibility of that organization. Outgoing distribution and official mail properly packaged and prepared for metering or distribution will be gathered internally within such offices and passed to the OMDC courier for further processing. A HWAD ACO government personnel will be appointed as the Official Mail Manager (OMM) and will oversee the operations of the OMDC.

- 7.1. Contractor personnel performing duties within the OMDC must meet the employee qualifications required in DOD 4525.8M, paragraph C.2.4.1. This includes a requirement to have an Interim Secret clearance or be eligible for a Secret clearance based on having a favorable Entrance National Agency Check (ENTNAC) or National Agency Check (NAC) on file.
 - 7.1.1. In CONUS, first class mail endorsed Return Services Requested, certified mail, and/or registered mail may contain classified material. Since Official Mail and Distribution Center personnel are authorized to open this mail if necessary for security reasons or to determine proper address, these individuals cannot simply be eligible for a clearance but must possess a secret clearance.
- 7.2. The contractor shall provide mail delivery and pickup service for the HWAD ACO staff once a day on each normal working day at a single designated mail drop at the HWAD administrative office.
 - 7.2.1. Delivery of incoming USPS mail for the HWAD ACO staff shall be within one hour after receipt of the incoming USPS delivery.
 - 7.2.2. Outgoing mail shall be processed by the OMDC in order to be included in the next daily pickup by the USPS.
- 7.3. The contractor shall be available to provide assistance to the OMM in conducting OMDC inspections and correcting any deficiencies in the operations of the OMDC.
 - 7.3.1. At a minimum, the OMM will conduct annual inspections as required by DoDI 4525.8 paragraph E4.3.4. and AR 25-51 paragraph 1-6.c.(3). Other inspections from higher headquarters, Army, DoD, and/or the USPS may occur. The contractor

shall be available to provide assistance in all OMDC inspections.

7.3.2. The contractor shall remedy any/all deficiencies that were detected during OMDC inspections. Timelines for correcting deficiencies will be determined at the conclusion of the inspections and will be based on the urgency/importance of the deficiency.

7.4. Contractor employees performing OMDC duties shall complete all applicable training as required in DoDI 4525.08.E4.3.2. Training can be accomplished on-line at the GSA Mail Management Overview website (www.gsa.gov/mailpolicy) or by attending the DoD Official Mail Workshop. The installation OMM will provide guidance to contractor employees to ensure this training is completed within the timelines stated below.

7.4.1. The contractor shall at least one OMDC employee fully trained by the time these duties are to be performed under this PWS. The contractor shall maintain at least one fully trained OMDC employee throughout the performance of this contract.

7.4.2. New contractor OMDC employees shall complete the required training within four months of assignment to the OMDC duties.

7.5. The Contractor will ensure that protective clothing is available when suspected chemical/biological agents are introduced into the mail inspection areas. The contractor will take appropriate security and medical actions in the event a mail handler is suspected of being contaminated.

7.6. The Contractor shall use the government furnished x-ray detection device to detect explosive devices before sorting is conducted in accordance with DA PAM 25-52 Section IV. The contractor shall furnish training to ensure all official mail personnel using x-ray equipment can recognize threat mail.

8. Transition/Phase out:

8.1. At the conclusion of this contract, if appropriate, a transition phase will start no later than (60) days prior to the expiration date of this contract. The contractor shall remain responsible for the full performance of all efforts identified in this work statement and will cooperate fully with the HWAD staff and/or the incumbent contractor.

8.2. The contractor shall identify all user accounts and provide administrator account access to supported information systems to the HWAD IAM or designated ACO staff member.

8.3. At the conclusion of the current contract, the incumbent contractor shall assist the HWAD IAM to validate system access levels of all user accounts on the government IS.

8.4. The IT products of Army-related work are the property of the U.S. Government, regardless of the ownership of the automation hardware or software used to create the products. The contractor shall fully cooperate in providing all documentation and data

identified by the government as government owned information. Final Disposition of Reports, Charts, Logs, and Maps. All reports, charts, logs, and maps shall become the property of the Government upon completion or termination of the contract and shall be available for inspection by the Government upon request at any time during the performance period. Any Government publication provided to the PA during its performance under this contract shall be returned to the Government. Manufacturer's brochures and warranty materials obtained by the PA, incidental to the performance of the PWS, shall be turned over to the Government upon completion or termination of the contract. Records relating to the normal accomplishment of a task or a mission are required to be filed by the respective contract paragraph number in chronological order. Disposition of all records shall be the responsibility of the Government.

9. An IT plan is required and will be evaluated as discussed in Attachment 0020, Section L of the solicitation.

10. Reference Documents:

Note: References 10.1 thru 10.4 are posted on the Army Publishing Directorate web page:

http://www.apd.army.mil/USAPA_PUB_pubrange_P.asp

- 10.1. AR 25-1 Army Information 4 Dec 2008
- 10.2. AR 25-2 Information Assurance 24 Oct 2007
- 10.3. AR 25-51 Official Mail and Distribution Management
- 10.4. DA PAM 25-52 Mail Facility Security and Handling Suspicious Mail
- 10.5. AR 380-67 Personnel Security 09 Sep 1988
- 10.6. DA PAM 25-1-1, Information Technology Support and Services 25 Oct 2006
- 10.7. Office of the Secretary of Defense, Memorandum, dated 16 Jan 2001, Subject: Common Access Card (CAC). <http://www.dtic.mil/whs/directives/corres/pdf/cio011601cac.pdf>
- 10.8. DoD Directive 8570.1 (DoDD 8570.1) Information Assurance Training, Certification, and Workforce Management, 15 August 2004. <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>
- 10.9. DoD 8570.01-M – Information Assurance Workforce Improvement Program, dated 19 December 2005. <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- 10.10. DoD 4525.8-M, DoD Official Mail Manual: <http://www.dtic.mil/whs/directives/corres/pdf/452508m.pdf>
- 10.11. DoDI 4525.08, DoD Official Mail Management <http://www.dtic.mil/whs/directives/corres/pdf/452508p.pdf>

10.12. Army Information Assurance Best Business Practice (IA BBP), 05-PR-M-0002, Training and Certification, Version 3.0.



IA Training &
Certification BBP Ver :

10.13. Department of the Army, Chief Information Officer/G-6, Memorandum dated 15 Aug 2006, Subject: Army Establishes Army Golden Master (AGM) as the Standard for Common Operating System Baseline Configurations.



AGM CIO G-6
Memo.pdf

10.14. List of Army Golden Master (AGM) version software roadmap.



AGM_Application_Ro
admap_8_6_30Jan_2

10.15. NETCOM Technical Authority (TA) Implementation Memorandum 2003-005c, Army Enterprise Desktop Standardization.



TA 2003-005c Army
Enterprise Desktop St

10.16. U.S. Army Networkiness Certification Program for Information Systems (Draft), 1 Aug 2007.



TA 2007-001
Networkiness Certifi