DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

26 JUL 2005

SAIS-GKM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Employment of Collaboration Capabilities Procedures

1. References.

a. Memorandum, Army Knowledge Management Guidance Memorandum Number 1, 8 Aug 2001.

b. AR 25-1, Army Knowledge Management and Information Technology Management, 30 Jun 2004.

c. AR 70-1, Army Acquisition Policy, 31 Dec 2003.

d. DOD Instruction 5200.40 DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 1997.

e. DOD Instruction 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003.

f. AR 25-2, Information Assurance, 14 Nov 2003.

g. AR 380-5, Department of the Army Information Security Program, 29 Sep 2000.

h. DOD Directive 5500.7-R, Joint Ethics Regulation (JER), Aug 1993.

i. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, 6 Jun 2003.

j. AR 340-21, The Army Privacy Program, 5 Jul 1985.

k. DOD Memorandum, CIO, subject: DOD Net-Centric Data Strategy, 9 May 2003.

2. This memorandum establishes Army procedures on the acquisition and implementation of Army collaboration capabilities to be deployed on the Army

Enterprise network or at local enclaves or domain levels. Collaboration capabilities are defined as the wide range of structures, processes, procedures, and services or tools necessary to enable two or more individuals who are not co-located to use an electronic synchronous or asynchronous environment to communicate, plan, coordinate and make decisions to achieve an objective. This procedure applies to the Active Army, the U.S. Army National Guard, the U.S. Army Reserve, U.S. Army civilians, and applicable U.S. Army supporting contractors.

3. Collaboration across the Army Enterprise and in a Joint, Inter-agency and Multi-national environment is critical to the Army's Joint Expeditionary Mindset. Collaboration enables our Forces to rapidly plan operations, exchange combat experiences, disseminate lessons learned, proven practices, and propagate operationally sound sustainment practices through the Modular force to the Power Projection/Support Platforms.

4. Army organizations will use the enterprise collaboration services and tools on Army Knowledge Online (AKO) to the greatest extent possible. AKO is the Army's integrated Enterprise portal and is an essential underpinning of the Army's transformation to a net-centric, knowledge-based force.

5. As the Core Enterprise Services Domain Lead, the Army CIO/G-6 is responsible for the development, operations, and maintenance of AKO and works in consultation with the AKO Capabilities Control Board (CCB). The AKO CCB was granted a charter by the Army CIO Executive Board (EB) to prioritize requirements for implementation of enterprise collaboration services and tools.

a. Army organizations and systems developers will submit their collaboration requirements to their Army CIO EB representatives to ensure consistency with their functional proponents' or commands' collaboration strategy and overarching requirements. These requirements need to be included in each functional area IT portfolio to be managed against competing requirements.

b. Upon validation and submission by their Army CIO EB representative, the requirements will be reviewed by the Knowledge Management Division, Governance, Acquisition and Chief Knowledge Office Directorate, CIO/G-6, and evaluated for enterprise-wide implementation. Fully vetted requirements will then be reviewed and prioritized by the Army AKO CCB and scheduled for implementation based upon resources, policy, and technology implications.

6. Because all requirements are not, by nature or scope, applicable to the Army enterprise, Army organizations and systems developers may have collaboration requirements that are not met through AKO validated by their organization and submitted through their Army AKO CCB representative. Prior to obtaining additional collaboration services and tools, regardless of whether IT or non-IT dollars will be expended, Army organizations and systems developers must work with their senior

information management officials (e.g., Chief Information Officers (CIOs), G-6's, etc.) to obtain all necessary waivers and/or approvals. This pertains to all collaboration tools and services regardless of dollar value or source. For non-IT funding of collaboration services or tools, an Army Knowledge Management (AKM) Goal 1 Waiver is required. AKM Goal 1 Resource Execution Guidance is issued by the Information Resource Integration (IRI) Directorate, Army CIO/G-6. Additional information is available on AKO on the IRI Homepage. The AKM Goal 1 Waiver process point of contact is Mr. Steven Smith at (703) 602-7900, steven.smith9@us.army.mil.

7. The Army Enterprise Infostructure Technical Configuration Control Board (AEI Tech CCB) will maintain a list of Enterprise collaboration tools and services on the Approved Products List (APL), located on the AKO AEI Tech CCB Homepage. Army organizations and systems developers may use tools on the APL if deployed in accordance with the approved configuration and implementation processes. If the collaboration tools and services will be used across the Army Enterprise Network and are not found on the APL, the proponent must use the Request For Change (RFC) process to introduce the tool and service for consideration into the AEI Tech CCB. For more information, contact AEI.TechCCB@us.army.mil.

8. For collaboration tools or services not on the APL, Army organizations and system developers will:

a. Ensure that the collaboration service or tool is certified by the Joint Interoperability Test Command (JITC) or has obtained a DOD Collaboration Interoperability Testing Program Statement of Non-Applicability (reference AR 25-1, paragraph 6-2). The point of contact for JITC testing is Mr. Robert Bouvier at (301) 744-2698, and a list of certified products can be found at http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html.

b. Obtain Intra-Army Interoperability Certification where applicable (Reference AR 70-1, chapter 7).

c. Obtain Information Assurance (IA) certification as per DODI 5200.40 (DITSCAP) implementing IA Controls in accordance with DOD 8500.2 (Information Assurance Implementation) and AR 25-2. The Army approving authority for IA certification is the Director of the Office of Information Assurance and Compliance (OIA&C, NETC-EST-I). Upon approval, the certification is submitted along with the software to the organization that will host the service.

d. Upon receipt of the IA certification, the hosting system/network will:

(1) update and obtain Designated Approval Authority (DAA) approval on the existing system/network accreditation to include the new capability using the OIA&C IA certification memo as IA certification documentation. For tools or services deployed on the Army Enterprise Network, the enterprise DAA is the Director for Enterprise System

Technology Activity (NETC-EST-D). For more information contact IACORA@us.army.mil;

(2) follow guidance contained in the Networthiness Implementation Plan to obtain Networthiness Certification from the U.S. Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC). For more information, contact army.networthiness@us.army.mil or (520) 533-4994, DSN 821. Networthiness Checklist Procedures and other applicable documents are available on AKO on the Networthiness Homepage. Tools currently in use that do not have, at a minimum, an Interim Authority to Operate (IATO) have 30 days from the date of this memorandum to obtain an IATO or migrate to an approved product.

e. Link the collaboration tool or service to AKO through Single Sign On (SSO). AKO currently provides the only authoritative Army Enterprise directory and the ability to manage identities, profiles and key information at the Enterprise level. Information and instructions on executing AKO SSO, including forms and technical platform requirements, are available on AKO. Linking to AKO through SSO does not currently apply to hardened tactical systems that exchange information or capabilities being deployed in bandwidth constrained tactical environments. For collaboration capabilities already in place for which there is no current technical solution to enable SSO, a waiver, to include a migration plan, must be obtained from the Knowledge Management Division, Army CIO/G-6.

9. Investments in collaboration services and tools should use the established DOD/Army Enterprise Agreements through the Army Small Computer Program Office (ASCPO) as per AR 25-1, paragraph 6-2. The existence of an Enterprise agreement does not signify approval for use on Army systems and the Army network. The Army organization or systems developer purchasing products through the ASCPO are responsible for ensuring that the services and tools comply with the policies and procedures outlined in this memo. Available Enterprise Agreements can be accessed at the ASCP website http://pmscp.monmouth.army.mil.

10. When using collaboration services and tools, Army organizations will adhere to all usage policies and guidlines established for information technology and communications systems. This includes, but is not limited to, the requirement of commanders and supervisors to:

a. Develop acceptable use policies for all users under their control (AR 25-1, paragraph 6-1).

b. Develop local policies and procedures on access control and management of information used in collaborative efforts (AR 25-1, 25-2, and AR 380-5).

c. Comply with configuration management and IA vulnerability management policies to maintain security of the collaborative environment over its entire lifecycle (AR 25-2).

11. All individual users are responsible for any communications and/or exchange and creation of information using collaboration capabilities and are subject to applicable professional, ethical and security guidelines (AR 25-1, AR 25-2, DOD 5500.7, AR 380-5, AR 380-10, and AR 340-21).

12. In addition to appropriately securing and managing access to collaboration services and tools and the content used and generated by collaboration activities, Army organizations and systems developers will follow all applicable content management and net-centric data strategies, policies and guidelines (DOD Net-Centric Data Strategy http://defenselink.mil/nii/doc/).

13. These procedures are effective immediately. Details of the processes identified in this memo will be made available at the Implementation of Collaboration Tools and Services site on AKO. The point of contact is Ms. Marlu Vance, (703) 602- 9635, marlu.vance@us.army.mil or Ms. Laura Petrosian, (703) 604-2019, laura.petrosian@us.army.mil.

STEVEN W. BOUTELLE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY)
ASSISTANT SECRETARY OF THE ARMY (CIVIL WORKS)
ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT AND COMPTROLLER)
ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE ARMY (MANPOWER AND RESERVE AFFAIRS)
GENERAL COUNSEL
ADMINISTRATIVE ASSISTANT TO THE SECRETARY OF THE ARMY
CHIEF INFORMATION OFFICER/G-6
THE INSPECTOR GENERAL
THE AUDITOR GENERAL
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
(CONT)

DISTRIBUTION: (CONT)
CHIEF OF LEGISLATIVE LIAISON
CHIEF OF PUBLIC AFFAIRS
DIRECTOR, SMALL AND DISADVANTAGED BUSINESS UTILIZATION
DIRECTOR OF THE ARMY STAFF
DEPUTY CHIEF OF STAFF, G-1
DEPUTY CHIEF OF STAFF, G-2
DEPUTY CHIEF OF STAFF, G-3/5/7
DEPUTY CHIEF OF STAFF, G-4
DEPUTY CHIEF OF STAFF, G-8
CHIEF, ARMY RESERVE
CHIEF, NATIONAL GUARD BUREAU
CHIEF OF ENGINEERS
THE SURGEON GENERAL
ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT
CHIEF OF CHAPLAINS
PROVOST MARSHAL GENERAL
THE JUDGE ADVOCATE GENERAL
SERGEANT MAJOR OF THE ARMY

COMMANDER
- U.S. ARMY EUROPE AND SEVENTH ARMY
- EIGHTH U.S. ARMY
- U.S. ARMY FORCES COMMAND
- U.S. ARMY TRAINING AND DOCTRINE COMMAND
- U.S. ARMY MATERIEL COMMAND
- U.S. ARMY CORPS OF ENGINEERS
- U.S. ARMY SPECIAL OPERATIONS COMMAND
- U.S. ARMY PACIFIC
- U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
- MILITARY SURFACE DEPLOYMENT & DISTRIBUTION COMMAND
- U.S. ARMY CRIMINAL INVESTIGATION COMMAND
- U.S. ARMY MEDICAL COMMAND
- U.S. ARMY MILITARY DISTRICT OF WASHINGTON
- U.S. ARMY SOUTH
- U.S. ARMY TEST AND EVALUATION COMMAND
- U.S. ARMY SAFETY CENTER
- U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND
- U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH ARMY SIGNAL COMMAND

PROGRAM EXECUTIVE OFFICER
- AMMUNITION
- AVIATION

(CONT)

DISTRIBUTION: (CONT)
AIR AND MISSILE DEFENSE
CHEMICAL AND BIOLOGICAL DEFENSE
COMBAT SUPPORT AND COMBAT SERVICE SUPPORT
COMMAND, CONTROL, AND COMMUNICATION SYSTEMS TACTICAL
ENTERPRISE INFORMATION SYSTEM
GROUND COMBAT SYSTEMS
INTELLIGENCE, ELECTRONIC WARFARE AND SENSORS
SOLDIER
SIMULATION, TRAINING, AND INSTRUMENTATION
TACTICAL MISSILES

PROGRAM MANAGER
JOINT PROGRAM OFFICE, BIOLOGICAL DEFENSE
CHEMICAL DEMILITARIZATION PROGRAM OFFICE
RESERVE COMPONENT AUTOMATION SYSTEM
JOINT TACTICAL UNMANNED AERIAL VEHICLES

DIRECTOR
ARMY ACQUISITION EXECUTIVE SUPPORT AGENCY
ARMY RESEARCH LABORATORY

CF:
COMMANDANT
U.S. ARMY LOGISTICS MANAGEMENT COLLEGE
U.S. MILITARY ACADEMY