AGM Program Change Request Process

U.S. Army Golden Master Program
NETCOM/ESD/EITS

Date 2/27/2009

Revision Sheet

Release No.	Date	Revision Description
0.0	8/25/08	Configuration Management Plan Initial Development
0.1	11/11/08	Updated processes for internal review
1.0	2/27/09	Initial Release

REFERENCES

a. CIO-G6 Memo, Army Establishes Source for Common Operating System Baseline Configurations, August 15th 2006

b. ALARACT 199/2008, 161739Z AUG 08, SUBJECT: MIGRATION TO MICROSOFT XP ARMY GOLDEN MASTER 8.0 AND VISTA ARMY GOLDEN MASTER 8.0

c. Federal Desktop Core Configuration Settings version 1.0, FDCC-Settings-major-version-1.0-062008.xls

d. OMB Memo, 1 June 2007, Subject: Ensuring New Acquisitions Include Common Security Configurations, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf

e. OMB Memo, 11 August 2008, Subject: Guidance on the Federal Desktop Core Configuration (FDCC), http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf

f. OMB Memo, 20 March 2007, Subject: Windows Common Security Configurations http://www.cio.gov/documents/Windows_Common_Security_Configurations.doc

g. AGM XP and Vista Security Baseline Configuration Spreadsheets, https://www.us.army.mil/suite/folder/1137580

h. Security Technical Implementation Guide (STIG), Windows 2000/XP/2003/Vista Addendum, V6R1 http://iase.disa.mil/stigs/stig/index.html

i. TECHNICAL AUTHORITY, Implementation Number 2003-005c, 13 September 2006, Army Enterprise Desktop Software Standardization.

j. Annex F (AGM Implementation) to HQDA EXORD 056-09 (Amplifying Guidance to USSSTRATCOM INFOCON 3, DTG221355ZNOV08)

2. PURPOSE

a. The purpose of this Document is to define the requirements to modify the Army Golden Master (AGM) baseline configuration and the change request/reporting process for organizational modifications.

b. This document defines the change request process referenced in the August 15th 2006 CIO-G6 Memo, Army Establishes Source for Common Operating System Baseline Configurations and ALARACT 199/2008, SUBJECT: MIGRATION TO MICROSOFT XP ARMY GOLDEN MASTER 8.0 AND VISTA ARMY GOLDEN MASTER 8.0.

3. SCOPE

a. The CIO G-6 memo, ALARACT 199/2008, and Annex F to HQDA EXORD 056-09/INFOCON 3 applies to all Microsoft Windows-based desktops and laptops within the Army Enterprise Infostructure (AEI). This includes program-based systems and stand-alone platforms not directly connected to the AEI.

b. The change request/reporting process is specifically focused on the security configuration settings defined by the AGM program. These settings are defined by the AGM Program as Cat 1, Cat 2, and Cat 3 on the OS specific configuration documentation. A change request is not required for changes to the core common user applications or the security patches included on an AGM releases.

4. BACKGROUND

a. AGM Security Baseline: The AGM Desktop Security profiles are based upon the Federal Desktop Core Configuration (FDCC) and the Defense Information Systems Agency (DISA) Gold configuration for the XP Professional and Vista Enterprise operating systems. The security guideline configurations were evaluated against functional requirements and set accordingly. There are deviations from the DISA STIG and FDCC contained in the Vista Enterprise and XP Professional configuration, which are documented against each release configuration and published on the AGM AKO Knowledge Center. The AGM platform should be scanned prior to network deployment and following the organizational scan schedule. ***Any open findings following the installation of an AGM release must be mitigated, addressed, or accepted by organizations deploying an AGM based platform***.

b. AGM Organizational-level Modifications: The AGM Program defines a minimum baseline intended to be applied to all US Army computers before network connectivity. An AGM configuration does not automatically apply every possible security setting defined by the FDCC and DISA Gold standard due to operational and functional considerations. Several settings are based upon local requirements and must to be defined by the organization deploying the AGM configuration. One example of a localization setting is to rename the local administrator account. These organizational settings are defined in a post-installation document. An organization using the AGM is expected to review and introduce changes to support their specific users (following the change request process defined by this document) and apply additional security deemed necessary by the organizational IA policy. **An Army organization can and is expected to increase the level of any AGM security setting if the increased security is supported by their operational environment.**

c. AGM Applications: The AGM Program provides and supports enterprise level office productivity applications. AGM releases provide options to install the supported applications with an approved enterprise level configuration. **Note: MS Internet Explorer is considered as part of the Vista or XP OS configuration, not a separate AGM application.** US Army organizations can alter the configuration of an AGM application to increase the level of security or make the application more efficient (e.g. adding a local OSCP responder location to the Army Enterprise Tumbleweed application). The AGM Program does not mandate the installation of a particular non-OS inclusive application version or configuration. This is considered to be the responsibility of the organization deploying the AGM application. However, there are other policies that will determine a particular version of a desktop application (e.g. Information Assurance Vulnerability Management (IAVM) or that may require an update to the network accreditation package for a particular configuration change to an application (e.g. DISA's Desktop Application STIG).

d. AGM Security Patches: The AGM Program does not replace the requirement to follow the current Information Assurance Vulnerability Alert Management (IAVM) process. The AGM XP and Vista baselines complement the IAVM process by providing a list of security patches that are current as of the time of product release. The security patch requirements are highly dynamic, often changing on a weekly basis. The security patches provided in AGM release provide a minimum level of security, but organizations using the AGM must scan the platform prior to network connectivity, install additional required patches, and maintain IAVM compliance after platform deployment. The AGM Program views updates to security patches as Category 3 changes, requiring only organizational approval.

e. Existing Platforms: The Active Directory (AD) deployment across the AEI supports the baseline desktop security configuration by providing the capability to enforce or manage the AGM defined security settings via Group Policy Objects (GPO). This is the recommended approach to deploying and managing AGM Desktop baseline configurations. The AGM Program provides an importable GPO designed to assist organizations develop a specific configuration that automatically applies any required functional modifications. Existing AGM platforms can be updated to a newer AGM configuration through the deployment of an organizational level GPO that applies the updated configuration. The AGM Program has posted migration guidance on the AGM Army Knowledge Online (AKO) site, https://www.us.army.mil/suite/page/130061.

f. AGM Configuration Categories:

1) Category 1 (Cat 1): Cat 1 settings are defined as critical and reducing the level of security in these settings may introduce a high level of risk or may not integrate with the established standards of the Army, DoD, or Federal policy. Many of Cat 1 settings are based upon the FDCC required configuration settings or are required for connectivity into the Army Active Directory. Requests to modify to Cat 1 settings must be submitted to the NETCOM/9TH ASC POC identified below.

2) Category 2 (Cat 2): Cat 2 settings form a second layer of configuration that contains critical and important settings that can be modified to support functional requirements. Cat 2 settings are considered to be highly recommended security settings and are usually defined by DISA as critical or important. The approving organization must report Cat 2 modification and justification to the NETCOM/9TH ASC POC identified below for tracking purposes.

3) Category 3 (Cat 3): Cat 3 settings are the final layer of configuration that contains settings that are directly intended to be modified to support local functional requirements. Cat 3 settings are considered to be recommended security settings and are usually defined by DISA as Important or Moderate. Cat 3 settings are also common modifications that are expected to support known requirements (e.g. Terminal Service configurations to support remote desktop requirements). The Cat 3 designation is also used to identify a change to a policy that was released after the AGM baseline was finalized. The approving organization does not need to report Cat 3 modifications to NETCOM/9TH

ASC, but must review and document each change if it is a deviation from DISA STIG or FDCC requirements.

4) Pre-approved FDCC changes: The AGM Help Desk will maintain a set of pre-approved FDCC deviations that are not applied in the default AGM configuration. These configuration changes would support a specific requirement scenario for a single or small set of computers and would be applied by at an organizational level. An update to the network accreditation package will be required, but no change requests would be submitted.

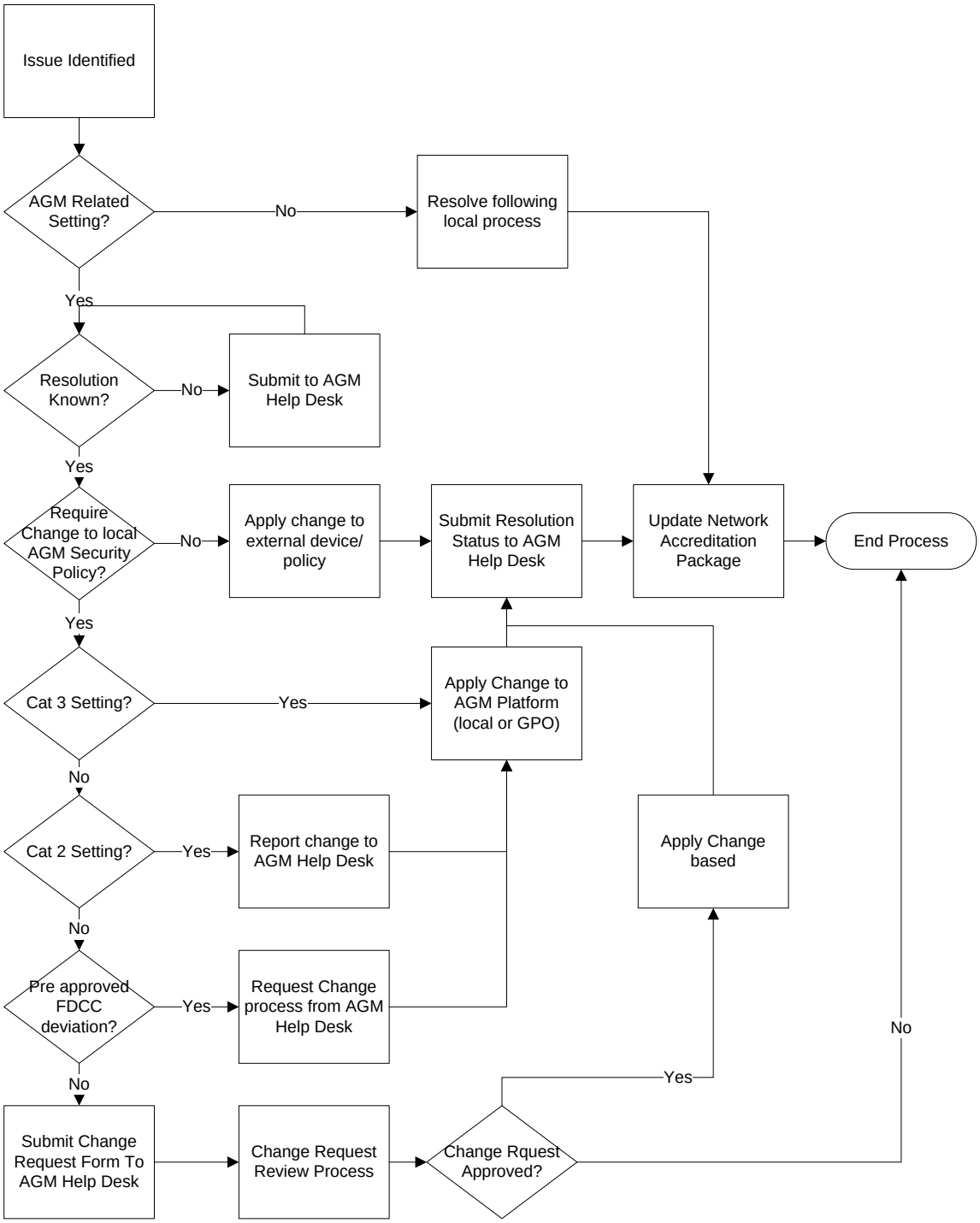
5. IMPLEMENTATION.

a. All organizations will begin analyzing the AGM Desktop configurations against the organizational network environment and functional requirements. The AGM Desktop configuration is directly associated with the FDCC and DISA Gold configurations and complies with the AR25-2 requirement directing that all information systems be compliant with DISA, Army, and NETCOM guidelines and have modifications fully documented and accepted by the appropriate DAA. The intent of the organizational analysis is to identify any required modifications to the AGM configuration to support organizational functional requirements.

b. Note: The AGM configuration that is deployed on an organizational production network must be approved by the organizational DAA even if no modifications have been introduced. The organizational network accreditation package must document the default AGM deviations and the DAA must accept the risk.

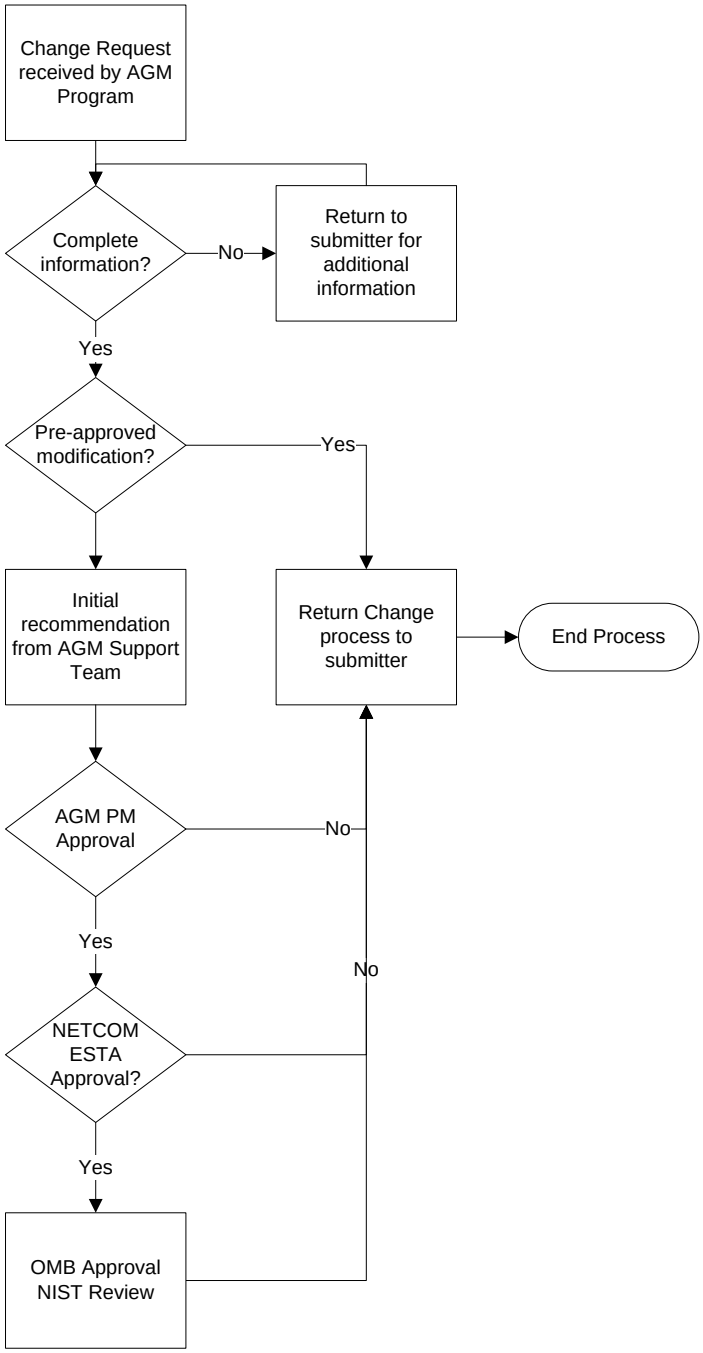
c. Deviation from the standard configurations identified in the AGM will occur in instances where unique mission requirements cannot be met using the standard configuration settings. AGM configuration settings can be modified by Directorates of Information Management (DOIM), Major Commands (MACOMs), Department of the Army (DA) agencies, Program Managers (PMs), or Program Executive Offices (PEOs) to support required processes and/or requirements. Organizations should determine the need for non-standard configurations considering mission requirements and a vulnerability assessment. The deviation approval process will vary depending upon the category of the change, *but in all cases require approval by the organizational DAA.*

d. Change Request Decision Process: The process for processing a change request is provided in the diagram below. The basic process is to identify if an issue is related to an AGM setting and determine a resolution. Once the resolution is determined and assigned a category, the appropriate process is followed.



e. AGM Change Request Review Process: When a request to change a Cat 1 (e.g. FDCC) setting is received by the AGM Program, it will undergo several Army reviews and ultimately be submitted to the Office of Management and Budgeting (OMB) and be reviewed by National Institute for Standards and Technology (NIST) for approval. This process may take 3-6 months to complete. Note: OMB policy recognizes that agencies may determine that settings in the FDCC are not practical. In the March 20th memorandum to Chief Information Officers, OMB instructed agencies to provide documentation to NIST of any deviations from

the FDCC and the rationale for doing so. Report FDCC compliance through your organization's CIO hierarchy. An agency or department CIO must report compliance for that organization.



6. <u>REPORTING FORMAT</u>

a. Cat 1: A Cat 1 modifications is intended to identify that a critical security setting in the AGM baseline configuration requires modification. A Cat 1 change should be expected to be approved at both the Army and Federal level (e.g. NIST and OMB) following the policy

published by OMB. A Cat 1 change request must include the change required to the Desktop configuration, the criticality of the mission impact that would result from not applying the change, the risk mitigation plan that the submitting organization is implementing for the modification, and the POA&M to remove the root cause of the mitigation (e.g. upgrading software). The submission should include a statement that the organizational DAA has approved all modifications that are being reported. **Cat 1 statements must be signed by the DAA or appointed alternate authority.**

b. Cat 2: Reporting of Cat 2 modifications is primarily intended for tracking purposes on the AGM program and will allow the AGM configuration to reflect an accurate representation of the US Army production environment. Every modification must include the justification and/or mitigation for the change. The submission should include a statement that the organizational DAA has approved all modifications that are being reported, but does not require a signature.

c. Resolution Status Reports to the AGM Help Desk: This process is intended to provide known workarounds and a status of pending issues to the AGM Program. These reports will allow the AGM Help Desk to maintain a list of common issues/resolutions to support future requests.

7. POINTS OF CONTACT:

a. AGM Policy POC:
   1) Shirley Dixon NETCOM\ESD\EITS
      a) Shirley.dixon@us.army.mil
      b) 703-602-0235

b. AGM Technical POC and Change Request Submission:
   1) AGM Help Desk
      a) agm.support@us.army.mil
      b) 1-800-966-7176