U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

# DEPARTMENTAL REGULATION	**Number: 3640-001**
SUBJECT: **Identity, Credential, and Access Management**	**DATE:** December 9 , 2011
	OPI: Office of the Chief Information Officer

TABLE OF CONTENTS

INTRODUCTION

1. PURPOSE

This Departmental Regulation (DR) establishes policies related to identity, credential, and access management (ICAM) for unclassified systems in the United States Department of Agriculture (USDA). This DR describes the policies, roles, and responsibilities necessary to meet ICAM-related requirements in Homeland Security Presidential Directive 12 (HSPD-12), National Institute of Standards and Technology (NIST) 800-53, NIST SP 800-63, Office of Management and Budget (OMB) M-04-04, OMB M-11-11, and OMB Circular A-123, Appendix A. This DR also aligns USDA policy with federal guidance and programs, such as the Federal ICAM Roadmap and Implementation Guidance. Additional departmental guidance is contained in DR/Departmental Manual (DM) 4620-002. These and other authorities and references are provided in Appendix A.

The goal of this policy is to provide a consolidated approach for all Department-wide ICAM activities to ensure consistency, uniformity, alignment, clarity, and interoperability.

2. BACKGROUND

USDA's ICAM transformation is a part of a larger Government-wide mandate to increase security, facilitate online transactions, and improve access services and interoperability between the Government and its business partners and constituents.

USDA's ICAM program comprises the projects, processes, technologies, and supporting personnel used to manage identities, credentials and access to USDA applications, systems, and services. The purpose of the USDA ICAM program is to develop and deliver centralized comprehensive technologies and business processes that manage identities, credentials, and access in order to establish a foundation for trust and interoperability in conducting electronic transactions.

The goals of the USDA's ICAM program are to streamline collecting and sharing of digital identity data, fully leverage personal identity verification (PIV) and PIV-interoperable credentials, enhance the physical access control system (PACS) infrastructure, modernize the logical access control system (LACS) infrastructure, and support federated identity capabilities.

USDA's HSPD-12 Program, as outlined in DR/DM 4620-002, facilitates the PIV credential management process by identity proofing, vetting, enrolling, tracking, and issuing credentials to applicable personnel. DR/DM 4620-002 also allows for other credentials such as an alternative PIV and Site Badges for personnel not required to be issued a credential.

The ICAM program encompasses a variety of business processes, systems, and subsystems. The Enterprise Entitlements Management Service(EEMS) is a major system that encompasses several subsystems, including the USDA eAuthentication Service, the Enterprise Directory, and others.

3. SPECIAL INSTRUCTIONS, APPLICABILITY, AND CANCELLATION

The policies, roles, and responsibilities described in this DR are applicable to all USDA agencies for both federal employees and non-federal employees, and are supported by detailed processes, procedures, and requirements that are described in the associated ICAM Departmental Manuals (DMs).

In the event that unclassified legacy and special purpose systems cannot use enterprise ICAM services, an extension request (Appendix B) must be submitted and approved following the procedures described in the ICAM DM. Extension requests are only approved for a limited period of time; the time period will be specified in the approval memorandum.

In addition to setting policy for ICAM in USDA, this DR supersedes DR 3610-001, USDA eAuthentication Service, in its entirety.

This DR will be in effect until superseded. If any provision of this DR is superseded by an official USDA memorandum or otherwise invalidated by external laws, directives, or standards, such invalidity does not affect other provisions of this DR. In the event of reorganization of offices or mission areas, USDA must ensure each of the roles and responsibilities described in this DM are specifically assigned to a new or existing organization or team.

4. ABBREVIATIONS AND DEFINITIONS

Agency or agencies - USDA mission areas, agencies, and offices

Authoritative system - system designated by USDA to be the official primary source for identity-related records, data, or attributes; such a system may or may not be a system of record.

Enterprise directory services - an enterprise-level directory of all identities in USDA maintained for logical access purposes, similar in structure and purpose to an agency active directory.

Federal employees - persons employed by USDA who act on behalf of USDA and need access to USDA facilities and systems, and therefore have an authoritative identity record in USDA ICAM systems.

Identity lifecycle management - the creation, administration, maintenance, and disposition of a digital identity.

Non-federal employees - persons who are not employed by USDA (e.g., contractors, affiliates, partners, volunteers, et al.). If act on behalf of USDA and need access to USDA facilities and systems, have an authoritative identity record in USDA ICAM systems.

Non-USDA federal employees - employees of other federal agencies who could be granted access to USDA systems and/or facilities.

PIV credential - personal identity verification cards or other form factors that comply with Federal Information Processing Standard (FIPS) 201 or superseding standards.

Refer to DM 4620-002, *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*, for more detailed definitions. This DR does not address identity, credential, or access management for persons with non-employee type relationships with USDA, such as customers, employees of customers, partners, service providers, and others.

CHAPTER 1

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT POLICY

1. GENERAL

a. Departmental agencies must comply with federal ICAM program objectives for all applicable USDA federal employees and non-federal employees who work for USDA.

b. The Enterprise Entitlements Management Service (EEMS) is the official system for synchronizing identity data from authoritative sources to consuming systems. For all new USDA systems in development or existing systems being upgraded, receipt of identity-related data from authoritative systems must be done via EEMS. For USDA systems that currently use legacy authoritative sources for identity data, any upgrades to the system must also include conversion to use EEMS instead of the legacy data source.

c. USDA agencies must use the USDA eAuthentication Service, a component of EEMS, to implement authentication and authorization capabilities for all Web-based applications. The USDA eAuthentication Service provides authentication and authorization services for USDA Web-based applications. Authentication confirms a person's identity, based on the reliability of his or her credential; authorization identifies the person's user permissions. This policy applies only to web-based applications; it does not apply to client/server, mainframe, desktop, network or other legacy application architectures. Using the USDA eAuthentication Service enables Web-based applications to support the use of PIV credentials.

d. For all new USDA systems in development that make use of user credentials, authority to operate may only be granted for systems that support the use of PIV credentials.

e. For all existing PACS and LACS, any upgrades to the system must be HSPD-12 compliant and compatible with the ePACS environment as well as support the use of PIV credentials.

f. USDA must procure services and products involving PACS and/or LACS that comply with HSPD-12 policy and Federal Acquisition Regulations and be on the GSA Approved Products List.

g. The Federal Chief Information Officers Council's Federal Identity Credential Access Management (FICAM) Roadmap and Implementation guidance must be used as a reference source when planning and implementing USDA ICAM activities, projects, and business processes.

2. ICAM GOVERNANCE

a. USDA's ICAM program is an enterprise-level approach that requires management, maintenance, and continual improvements to meet regulatory requirements and USDA's goals to realize improved efficiencies and cost savings for ICAM-related processes and controls. Therefore, USDA must establish and maintain an ICAM Steering Committee, sponsored by the USDA Chief Information Officer and made up of key stakeholders in USDA. The ICAM Steering Committee governance structure, functions, roles and responsibilities are described in future ICAM DM**.**

b. USDA must maintain an enterprise-level ICAM Program Office to manage and administer the program. Additionally, the ICAM Program Office is responsible for daily operations, maintenance, and integration support of the enterprise ICAM systems.

c. USDA agencies must establish and maintain an agency ICAM team that is responsible for planning, coordinating, and implementing agency-specific ICAM initiatives, directives, and activities, and for communicating processes and procedures to its user population.

3. IDENTITY MANAGEMENT

a. USDA's ICAM program must support identity life-cycle management, identity maintenance, and enterprise directory services.

b. In USDA, a person's digital identity record must be used for the lifetime of the person. Just as each individual has a unique set of characteristics that make the individual unique, each individual may have only one USDA digital identity record.

c. ICAM services ensure that people are properly vetted based on their affiliation with USDA and the USDA facilities and systems to which they require access. USDA ICAM services must provide the ability to create, modify, vet, and retire the identities of people who access USDA facilities and systems through the approved identity authoritative source.

d. USDA's ICAM service must support the management of federated identity records from trusted identity providers both within and outside the Federal Government.

e. USDA ICAM identity records must be made available through and to approved USDA systems and directories to support USDA agencies and the conduct of USDA business.

f. USDA must create and maintain a standardized core attribute list that constitutes the minimum requirements for a single digital identity record for each person in USDA, and each authoritative USDA digital identity record must include these attributes. USDA must create and maintain a current list of the authoritative data source for each attribute on the core attribute list.

g. All non-federal employees who access USDA physical or logical systems must be entered into the USDA approved identity management or authoritative system for such persons for complete identity and credential management. This process also supports the issuance of alternative PIV and Site Badges.

h. To meet OMB requirements, USDA must use the Office of Personnel Management's (OPM's) Clearance Verification System (CVS) or designated successor system before conducting a background investigation. USDA must also enter background investigation results for all federal and non-federal employees in the Department-designated authoritative system. Therefore, the USDA ICAM system will only accept background investigation or adjudication results from OPM or the USDA-designated authoritative system. Background investigation or adjudication information that is sent to other Federal Agencies must originate from the USDA authoritative source.

4. CREDENTIAL MANAGEMENT

a. USDA and agencies must assign credentialing roles as required in DR 4620-002, Common Identification Standard for U.S. Department of Agriculture Employees and Contractors.

b. USDA approved credentials are issued to allow access to both physical and logical assets throughout USDA. The ICAM Program Office must maintain a current list of approved PIV credentials used in USDA and supported by USDA systems.

c. USDA must ensure that Public Key Infrastructure (PKI) certificates for authentication, encryption, and signing operations are issued and maintained in accordance with the x.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

d. USDA certificate management services must provide PKI certificates for both persons and non-person entities.

e. USDA must create and maintain an authoritative attribute exchange service capability, referred to in this document as the Enterprise Entitlement Management Service (EEMS), as the means to securely share authoritative identity attributes and credentials within the department and its agencies.

f. USDA and agency personnel and systems must adhere to the processes, procedures, and rules defined in the ICAM DM for data access and sharing, and appropriate use of identity-related data in ICAM systems.

g. For connections to/from ICAM systems to USDA and agency systems, system owners must meet the requirements defined in and agree to rules of engagement described in the ICAM DM for such connections.

h. For federal employees and non-federal employees who need a PIV credential, USDA agencies must enter all new identities into authoritative data sources and verify completion of all information required to enroll for PIV credentials prior to entry on duty (EOD) date.

i. OMB requires that PIV credentials be used for access to all on-site systems by all permanent, on-site employees. As an interim path toward meeting OMB requirements, USDA uses "mixed mode" authentication, which allows access using either PIV credential or user ID/password within the USDA network.

5. AUTHORIZATION AND ACCESS

a. USDA ICAM systems must provide enterprise support and infrastructure for both physical (facility) and logical (network) authorization and access.

b. EEMS is USDA's officially designated system for ensuring the proper identification and registration of USDA access and the required attributes needed for authorization and access management in the department and agencies.

c. ICAM must support the authorization and access, including creation, modification, suspension, and disablement, of identities that require access to USDA LACS and PACS systems and infrastructure.

d. ICAM must supply authentication services to ensure that the person or non-person entity attempting to access a system matches an asserted identity and credential at the appropriate access level.

e. Non-person entities must be designated by USDA as a "trusted entity" to be granted access or authentication to USDA LACS or PACS.

f. USDA or agency systems must comply with applicable FIPS, NIST, and OMB standards (See Appendix A, Authorities and References) in order to be approved for integration with ICAM systems. Only USDA applications and systems that uniquely identify and authenticate all users will be approved to integrate with ICAM systems.

g. USDA, through its ICAM program, will develop and implement an enterprise approach for providing privileged account and password management, including

enabling the ability to manage provisioning and deprovisioning of these account types, lifecycle management of privileged accounts and passwords, and system accounts.

6. AUTHENTICATION

a. The ICAM program must support EEMS's USDA eAuthentication Service, which provides authentication and authorization services for USDA Web-based applications. Authentication confirms a person's identity; authorization identifies the person's user permissions.

b. USDA agencies must use the USDA eAuthentication Service to implement authentication and authorization capabilities for all Web-based applications, regardless of whether the users are external or internal. This policy applies only to Web-based applications. It does not apply to client/server, mainframe, desktop, network, or other legacy application architectures.

(1) USDA Web-based applications requiring authentication must integrate with the USDA eAuthentication Service to provide user authentication functionality.

(2) USDA Web-based applications must leverage the USDA eAuthentication Service to provide coarse-grained authorization when appropriate attributes/roles exist.

(3) USDA Web-based applications must create fine-grained authorization controls in the application when required by the business function.

c. The USDA eAuthentication Service must support the following concepts: Credential Assurance Levels; Authentication Risk Assessment; Credential Management; Site Protection; Records Management; Privacy Protection; and Training.

d. USDA's systems must use the identity authentication assurance levels defined by OMB and NIST for USDA electronic government services, and as detailed in the ICAM DM(s). USDA agencies are responsible for determining the required level of assurance for authentication for each business transaction.

e. For all USDA and agency Web-based applications, users will use the credentials provided and/or approved by the USDA eAuthentication Service. These credentials include:

(1) Levels 1 & 2: User IDs and passwords for federal employees, non-federal employees, customers, and affiliated users.

(2) Levels 3 & 4: PKI credentials for federal employees and non-federal employees that are issued by USDA HSPD12 program (e.g., PIV credentials).

(3) Levels 3 & 4: PKI credentials for customers and affiliated users issued by USDA-approved credential service providers.

f. USDA will provide a federated foundation for supporting Agencies in federation initiatives and systems. ICAM will provide one or more solutions for federation to enable USDA to accept and supply trusted identities and/or credentials provided and managed by federated identity providers (IdPs) and credential service providers (CSPs), as needed, to support USDA's ICAM mission.

7. CRYPTOGRAPHY AND DIGITAL SIGNATURE

a. Agencies must enable use of the PKI certificates associated with a USDA-approved PIV credential to digitally sign and encrypt emails, business transactions, and relevant business documents in those cases where digital signatures and/or encryption are required.

b. Individuals who have been issued PIV credentials and who are required to provide a digital signature must use the PIV credential. The PIV credential uses PKI technology to ensure authentication of both document content and signature.

c. All USDA systems and applications with a security requirement for non-repudiation of a document or transaction must use digital signatures for this purpose.

8. AUDITING AND REPORTING

a. ICAM systems must support complete logging and audit trails for creating, modifying, or deleting identities, accounts, and access privileges.

b. ICAM systems must support the reporting necessary to enable periodic compliance reviews of access for identities requiring access to USDA’s facilities and systems.

CHAPTER 2

ROLES AND RESPONSIBILITIES

1. DEPARTMENT MANAGEMENT

Department Management has roles and responsibilities in ICAM, and must, in

collaboration with OCIO, ensure that ICAM program services for using and integrating ICAM are implemented in compliance with applicable laws, regulations, and USDA program directives and requirements.

2. OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)

OCIO and its divisions/branches have roles and responsibilities in ICAM, and must:

a. Sponsor, establish and maintain an ICAM Steering Committee.

b. Provide an enterprise-level ICAM infrastructure to support managing identities, credentials, and access to USDA and agency applications, systems, and services.

c. Establish and maintain an ICAM Program Office to manage and administer the USDA ICAM program and to be responsible for daily operations, maintenance, and integration support of the enterprise ICAM infrastructure.

d. Publish and maintain the ICAM DM(s), guidance, handbooks, which will provide detailed information and guidance about the use of systems and processes to meet the requirements in this ICAM policy.

e. Serve as system owner of the ICAM infrastructure, and provide or establish system service-level agreements and interconnection security agreements with owners of connecting systems.

f. Operate enterprise ICAM systems in compliance with USDA security requirements, and be responsible for certification and accreditation efforts.

g. Manage and protect identity information provided by USDA-designated authoritative systems, and manage the enterprise directory services.

h. Create and maintain a standardized core attribute list that constitutes the minimum requirements for a single digital identity record for each person in USDA.

i. Create and maintain a current list of the authoritative data source for each attribute on the core attribute list.

j. Review and approve or deny extension requests for systems or processes that cannot be aligned to the ICAM program directives, and track progress toward compliance.

3. CYBER POLICY AND OVERSIGHT (CPO)

CPO has roles and responsibilities in ICAM, and must:

a. Participate on and supply a representative to the ICAM Steering Committee in USDA, and offer in consultation ICAM program, policy, and process direction for cyber policy and oversight activities and responsibilities.

b. Consult with the Office of the Chief Information Officer (OCIO) and the Agriculture Security Operations Center (ASOC) to establish policies, standards, and procedures for implementing and administering the ICAM program throughout USDA.

c. Review and consult on all ICAM program audit and compliance activities, including ICAM system artifacts that will be submitted for audits from agency ICAM integrated systems.

4. OFFICE OF HOMELAND SECURITY AND EMERGENCY COORDINATION (OHSEC)

OHSEC has roles and responsibilities in ICAM, and must:

a. Participate on and supply a representative and alternate to the ICAM Steering Committee in USDA, and offer in consultation ICAM program, policy, and process direction for homeland security and emergency coordination activities and responsibilities.

b. Collaborate with the ICAM Program Office in maintaining the official list of USDA-approved PIV credentials that support PACS and LACS in USDA.

c. Maintain an enterprise PACS structure in USDA and provide assistance and support to integrate it with EEMS. Collaborate with OCIO on Requests for Extension concerning legacy PACS and ePACS Configuration Management issues.

d. Manage and support PIV credential issuance and usage for USDA federal employees and non-federal employees. Facilitate Interagency Agreement with GSA as USDA's HSPD-12 Service Provider.

e. Maintain DRs and DMs (e.g., DR 4620) to comply with the specific requirements of applicable federal laws, regulations, and standards, such as HSPD-12, FIPS 201, etc.

5. OFFICE OF HUMAN RESOURCE MANAGEMENT (OHRM)

OHRM has roles and responsibilities in ICAM, and must:

a. Participate on and supply a representative and alternate to the ICAM Steering Committee in USDA, and offer in consultation ICAM program, policy, and process direction for HR and human resource management activities and responsibilities.

b. Develop and issue USDA-wide policies and procedures to ensure that HR staff (Department, agency, or external services) that process new employees must capture and enter accurately and timely all identity information required for ICAM compliance.

c. Manage, maintain, and make timely changes as appropriate to identity-related data that is used for ICAM purposes or in ICAM-connected systems, to meet regulatory requirements, ICAM goals, and USDA objectives for improved efficiency, as described in the ICAM DM(s).

d. Collaborate with the ICAM Program Office to identify attributes in HR systems that will be designated as authoritative and be part of the standardized core attribute list that constitutes the minimum requirements for a single digital identity record.

e. Develop policies and procedures to ensure a background investigation has been initiated prior to EOD date for new employees and prior to the start date for new non-federal employees, and for allowing a PIV credential with a provisional status to be issued upon successful adjudication of an FBI fingerprint check.

6. OFFICE OF THE CHIEF FINANCIAL OFFICER (OCFO)

OCFO has roles and responsibilities in ICAM, and must:

a. Participate on and supply a representative to the ICAM Steering Committee in USDA, and offer in consultation ICAM program, policy, and process direction for financial management responsibilities.

b. Review and consult on all ICAM program audit and compliance activities, including ICAM system artifacts that will be submitted for audits from agency ICAM integrated systems.

7. AGENCY CHIEF INFORMATION OFFICERS (CIOs)

Agency CIOs have roles and responsibilities in ICAM, and must:

a. Comply with OMB FICAM, NIST's FIPS 201-1, the NIST guidance relevant to ICAM, and the ICAM DM(s).

b. Create, engage, and maintain an agency ICAM team, and report on ICAM implementation progress as directed by the ICAM Program Office.

c. Implement ICAM program services in compliance with all Federal and USDA regulations, and comply with USDA policies and procedures to support ICAM program processed for identity, credential, and access management.

d. Implement enhancements or new systems to ICAM program services to meet ICAM requirements for integration with USDA enterprise ICAM services as approved by the ICAM Program office.

e. Develop agency ICAM architecture roadmaps and implement ICAM program services in alignment with USDA ICAM enterprise architecture roadmap.

f. Ensure compatibility of agency PACS and LACS with USDA Enterprise PACS (ePACS), LACS, and ICAM systems, and comply with USDA PACS, LACS, and ICAM policies and procedures.

g. Use the ICAM infrastructure for the creation and maintenance of identity and credential information for all persons accessing USDA LACS and PACS.

h. Ensure that all persons accessing agency systems have a USDA-accepted identity, and that all relevant attributes have been appropriately completed.

i. Request extensions for systems or processes that cannot be aligned to the ICAM program directives.

8. USDA AGENCY ICAM TEAM PROJECT LEADS

Agency ICAM Project Leads have roles and responsibilities in ICAM, and must:

a. Work directly with the ICAM Program Office on all ICAM program activities.

b. Assist the Agency CIO with implementing ICAM in the agency, and provide all details when any service or systems will be integrated with or removed from the USDA ICAM system.

c. Serve as the primary coordinator for all ICAM-related activities in the agency, and prioritize ICAM implementations as directed by USDA leadership, agency leadership, and business needs.

d. Provide reports and data on the agency's ICAM implementation activities and progress as requested by the ICAM Program Office or as required by federal directive.

e. Determine the appropriate provisioning method to manage access to information under their authority, using the USDA ICAM program service using one of the following methods:

(1) An approval-based method for granting access to their information technology (IT) asset(s).

(2) An approved auditable access control process designation or other attribute based logic maintained authoritatively in ICAM services integration.

9. USDA FEDERAL EMPLOYEES AND NON-FEDERAL EMPLOYEES

USDA federal employees and non-federal employees (contractors, partners, affiliates, volunteers, et al.) have roles and responsibilities in ICAM, and must:

a. Notify their PIV credential sponsor and/or HR point of contact of any changes in identity information, such as legal name or citizenship status.

b. Use only the USDA-approved credential(s) for accessing PACS and LACS in USDA.

c. Not share their credentials and/or secret keys with another person.

d. Secure their credentials and secret keys in a way that reduces the likelihood that they will be used by others.

-END-

APPENDIX A

AUTHORITIES AND REFERENCES

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, November 10, 2009.

Federal Information Processing Standard Publication (FIPS PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006

FIPS PUB 186-3, *Digital Signature Standard (DSS)*, June 2009.

Government Paperwork Elimination Act (GPEA), U.S.C §3501 et seq.

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

National Institute of Standards and Technology Special Publication (NIST SP) 800-63, Revision 1.0.2, *Electronic Authentication Guideline*, April 2006 .

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations (*Errata as of May 1, 2010*)*, August 2009.

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control, Appendix A*, December 21, 2004.

OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003.

OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005.

OMB Memorandum, *Reciprocal Recognition of Existing Personnel Security Clearances*, December 12, 2005, and M-06-21, *Reciprocal Recognition of Existing Personnel Security Clearances*, July 17, 2006.

OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 30, 2006.

OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011.

The Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701 et seq.

The Electronic Signatures in Global and National Commerce Act, Public Law 106-229, June 30, 2000.

The Privacy Act of 1974, 5 U.S.C. §552a.

USDA DM 3530-003, *Use of Public Key Infrastructure (PKI)*, July 15, 2004.

USDA DM 4620-002, *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*, January 14, 2009.

USDA DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*, January 14, 2009, and draft update of June 27, 2011.

APPENDIX B

REQUESTS FOR EXTENSION

1. EXTENSION REQUESTS

Requests for extensions to implement the requirements of this DR may, at the discretion of the Department's Chief Information Officer, be granted to allow continued use of a legacy or special purpose LACS system that does not comply with the mandated requirements to use an approved method for identity, credential, and access, provided that:

a. There is a technological constraint that does not allow the use of or integration with the USDA enterprise ICAM services.

b. A transition plan is provided that details when the asset will be retired or integrated with the enterprise ICAM service.

c. The extension request is for an individual system or application; no blanket or group extension requests will be accepted or approved.

d. All granted waivers must have a time limit and an expiration date of no more than one year, and must not include an automatic extension clause. If the extension requires more time, a new extension request must be submitted and approved before the expiration date of the original extension. The extension request must be approved by the Department's Chief Information Officer. The extension request and approval process is described in the ICAM DM(s).

Refer to DM 4620-002 for the procedure for requesting an extension for a PACS system.