

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

DEPARTMENTAL REGULATION	NUMBER: DR 3640-001
SUBJECT: Identity, Credential, and Access Management	DATE: June 8, 2021
OPI: Office of the Chief Information Officer	EXPIRATION DATE: June 8, 2026

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Scope	3
4. Background	4
5. Policy	4
6. Roles and Responsibilities	8
7. Penalties And Disciplinary Actions For Non-Compliance	14
8. Policy Exceptions	14
9. Inquiries	15
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Definitions	B-1
Appendix C – Authorities and References	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) Identity, Credential, and Access Management (ICAM) policy for unclassified systems. This DR defines the authority for ICAM governance, policy, procedure, and technology.
- b. This DR complies with the requirements of the following:
 - (1) *Electronic Signatures in Global and National Commerce Act*, [Public Law 106-229](#);
 - (2) Office of Management and Budget (OMB) Memorandum [M-19-17](#), *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*;
 - (3) National Institute of Standards and Technology (NIST), Special Publication [\(SP\) 800-47](#), *Security Guide for Interconnecting Information Technology Systems*;

- (4) NIST, [SP 800-53 Revision 5](#), *Security and Privacy Controls for Federal Information Systems and Organizations*;
- (5) NIST, [SP 800-63-3](#), *Digital Identity Guidelines*;
- (6) NIST, [SP 800-157](#), *Guidelines for Derived Personal Identity Verification (PIV) Credentials*;
- (7) NIST, Federal Information Processing Standards Publication [\(FIPS PUB\) 186-4](#), *Digital Signature Standard (DSS)*; and
- (8) NIST, [FIPS PUB 201-2](#), *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR supersedes DR 3640-001, *Identity, Credential, and Access Management*, dated December 9, 2011.
- b. This DR is effective immediately when published and remains in effect until superseded or expired.
- c. This DR aligns with [DR 4620-002](#), *Common Identification Standard for U.S. Department of Agriculture*.
- d. Mission Areas, agencies, and staff offices will align their processes with this DR within 6 months of the publication date.
- e. If any provision of this DR is superseded by another Departmental Regulation or otherwise invalidated by external laws, directives, or standards, it does not invalidate nor affect other provisions of this DR.
- f. In case of reorganization, the USDA must ensure each of the roles and responsibilities described in this DR are assigned to another official, executive, or responsible individual.
- g. In this DR, the term “employee” or “USDA employee” refers to a Federal civil servant employed by, detailed or assigned to, the USDA, including members of the Armed Forces.
- h. In this DR, the term “personnel” or “USDA personnel” encompasses USDA employees, appointees, contractors, partners, affiliates, interns, fellows, and volunteers who work for, or on behalf of, the USDA, and whose work is overseen by USDA employees.

3. SCOPE

- a. This DR applies to all the following:
 - (1) USDA Mission Areas, agencies, and staff offices, including USDA personnel;
 - (2) Federal information, in any medium or form; generated, collected, provided, transmitted, stored, maintained; or accessed by; or on behalf of, the USDA;
 - (3) Information systems or services; cloud based, used or operated by, for, or on behalf of the USDA that is within a USDA accredited system boundary; and
 - (4) Facilities used by USDA from which these information systems or services operate, whether owned or operated by the USDA, or owned or operated on behalf of the USDA by a contractor, subcontractor, or other organization.
- b. This DR extends to the processes, procedures, and technology for any Information Technology (IT) system that requires management or authentication of an “identity.”
 - (1) For this DR, “identity” refers to the unique representation of a subject. This includes a person, a device, a Non-Person Entity (NPE), or an automated technology such as Robotic Process Automation (RPA). They must be engaged in a transaction with at least one Federal subject or resource; including data, information systems or facilities.
 - (2) This DR refers to “identity” in two contexts:
 - (a) Electronic Federal enterprise identity (or simply enterprise identity), which refers to the unique representation of personnel who act on behalf of the USDA; an enterprise user (such as a mission or business partner); a device; or a technology; that a Federal agency manages; and
 - (b) Public identity, which refers to the unique representation of a subject that a Federal agency interacts with; but does not directly manage. Public identity may also refer to a mechanism of trust used to render services to the American public or USDA partners and collaborators.
- c. Detailed supporting processes, procedures, and requirements will be described in forthcoming associated ICAM Departmental Manuals (DM).
- d. Nothing in this DR will alter the requirements for the protection of information associated with national security systems such as those identified in the [*Federal Information Security Modernization Act \(FISMA\)*](#), 44 United States Code (U.S.C.) 3551 § *et seq.*, or the policies, directives, instructions, or standards issued by the Committee on National Security Systems (CNSS); or the intelligence community.

4. BACKGROUND

Advances in technology enable more digital and business transactions; and they also provide the opportunity to improve service delivery. The USDA continues to modernize and consolidate IT infrastructure and services to improve efficiency, effectiveness, security, and customer experience. New challenges have emerged along with these advances; such as data breaches exposing controlled unclassified information (CUI); for example, passwords and Personally Identifiable Information (PII), in particular. Identity management has become even more critical to the USDA's successful delivery of services.

To ensure secure and efficient operations, the USDA must be able to identify, credential, monitor, and manage identities that access Federal resources; such as data, information systems, facilities, and secured areas. The USDA must be able to conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control. This significantly affects the security, privacy, and delivery of the USDA mission; and enhances the trust and safety of digital transactions with the American public.

The USDA ICAM transformation is part of a larger Governmentwide mandate to implement ICAM security disciplines. This will enable the right individual to access the right resources, at the right time, for the right reasons. The USDA ICAM program includes policy, processes, technologies, and personnel. Together, they identify, credential, monitor, and manage user access to information and information systems for the USDA.

5. POLICY

a. ICAM Governance.

- (1) ICAM requires an enterprisewide approach, to harmonize governance, architecture, and acquisition; and to ensure an efficient and effective implementation. To accomplish this, the USDA will establish an ICAM Program Office for the enterprise to:
 - (a) Manage, administer, maintain, and continually improve the program to meet regulatory requirements;
 - (b) Lead and synchronize ICAM implementation activities for all the USDA;
 - (c) Define, implement, and govern; the policy, processes, and technology solutions; to deliver enterprise ICAM capabilities to all the USDA; and
 - (d) Be responsible for daily operations, maintenance, and integration support; of ICAM shared services and enterprise capabilities managing digital identities, credentials, and access; to the USDA systems and applications.

- (2) The USDA ICAM Program Office must establish and maintain an ICAM Advisory Council. The ICAM Advisory Council will:
 - (a) Include the Chief Information Officer (CIO), the Chief Financial Officer (CFO), the Chief Information Security Officer (CISO), the Senior Agency Official for Privacy (SAOP), the Chief Data Officer, the Chief Acquisition Officer (CAO) and may include others as necessary;
 - (b) Include senior officials from the Office of Human Resource Management (OHRM), the Office of the General Counsel (OGC), and the Office of Safety, Security, and Protection (OSSP); and
 - (c) Adhere to the structure, functions, roles, and responsibilities, set forth in the ICAM Advisory Council Charter.
- (3) The USDA ICAM Program Office will establish and maintain an ICAM Cross Agency Working Group (CAWG). The ICAM CAWG will:
 - (a) Include ICAM liaisons from each Mission Area, agency, and staff office; to coordinate the implementation, management, and maintenance of ICAM capabilities;
 - (b) The function of the CAWG is to facilitate communication with stakeholders, enable the sharing of feedback, and coordinate ICAM efforts with USDA mission areas.
 - (c) Adhere to the structure, functions, roles, and responsibilities set forth in the ICAM CAWG Charter;
 - (d) Align ICAM services and management with USDA's mission;
 - (e) Establishes cross-team collaboration to provide guidance, identify common agency challenges, establish best practices, and share solutions;
 - (f) Ensures proper agency resource allocation to ICAM programs and projects;
 - (g) Reviews post-implementation evaluations to ensure that ICAM services and programs meet forecasted benefits and outcomes;
 - (h) Provides counsel to the ICAM Program Office to align ICAM technology, policy, and execution with USDA's overall mission;
 - (i) Advise, guide, and Support USDA Enterprise Risk Management capabilities to effectively guide enterprise ICAM efforts; and

- (j) Ensure ICAM processes, procedures, and technology solutions meet Mission Area, agency, and staff office requirements for mission delivery.
- (4) The USDA ICAM Program Office will outline performance expectations, including security and privacy risk management, throughout the identity lifecycle for the enterprise. These performance expectations must support the President's Management Agenda (PMA) Cross Agency Priority (CAP) goals.
- (5) As outlined in NIST SP 800-63-3, Mission Areas, agencies, and staff offices must incorporate Digital Identity Risk Management into their existing processes when working with ICAM integrations. ICAM integrations require an Interconnection Security Agreement (ISA) document. The ISA must be completed in compliance with the requirements of NIST SP 800-47.

b. ICAM Architecture.

- (1) The USDA ICAM Program Office must establish solutions for ICAM services and maintain a technology solution roadmap for the enterprise. ICAM solutions must adhere to the following:
 - (a) Align with the Federal Identity, Credential, and Access Management (FICAM) architecture, based on the [*Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance*](#), Version 2.0;
 - (b) Align with Continuous Diagnostics and Mitigation (CDM) requirements;
 - (c) Applicable Federal policies, standards, playbooks, and guidelines; and
 - (d) Publish in the [ICAM service catalog](#).
- (2) All USDA Mission Areas, agencies, and staff offices must use the following:
 - (a) Enterprise ICAM shared services to fulfill their ICAM requirements. Any exception to using Enterprise ICAM shared services must be approved using the waiver process.
 - (b) Enterprise ICAM shared services; for credentialing and identity proofing public consumers who require access to USDA digital services.
 - (c) The ICAM Enterprise Identity Management Service (EIMS) is the authoritative source for managing the digital identity lifecycle of all person identities. This includes all categories of USDA personnel, as well as public citizens who require authenticated access to the USDA online services.
 - (d) The ICAM EIMS is the authoritative source for managing the digital identity lifecycle of all NPEs. This includes service accounts and automated

technologies; such as RPA tools and Artificial Intelligence (AI). EIMS ensures the digital identity is distinguishable, auditable, and consistently managed.

- (3) All USDA systems or applications that store, maintain, or consume user accounts; must:
 - (a) Integrate with the ICAM EIMS to manage the digital identity lifecycle; and to enable compliance auditing and reporting;
 - (b) Establish processes to manage access control;
 - (c) Revoke access privileges when no longer authorized; and
 - (d) Revoke or destroy credentials in a timely manner, to prevent unauthorized access to information systems.
- (4) All USDA systems or applications that require authentication must use one of three approved enterprise authentication services, as appropriate, for the system use case;
 - (a) Enterprise Active Directory; for the USDA's domain for end user office automation services;
 - (b) Enterprise Data Center Active Directory; for the USDA's data center privileged system access; or
 - (c) eAuthentication Service; for all web and mobile application access, including internal users and public citizens.
- (5) All USDA Mission Areas, agencies, and staff offices must require the use of Homeland Security Presidential Directive [\(HSPD\)-12](#), *Policy for a Common Identification Standard for Federal Employees and Contractors*, compliant credentials by all federal employees and contractors. These credentials include, but are not limited to, the following:
 - (a) Personal Identity Verification (PIV) Credential;
 - (b) Personal Identity Verification Interoperable Credential (PIV-I); and
 - (c) Derived PIV (PIV-D) where applicable per Office of Personnel Management (OPM) requirements).
- (6) The HSPD-12 credentials serve as the primary means of identification and authentication to Federal information systems, federally controlled facilities, and other secured areas.

- (7) As technology evolves, the USDA ICAM Program, in cooperation with the Information Security Center (ISC), will review or approve Mission Area, agency, and staff office specific implementation of additional credential solutions. These must meet the intent of HSPD-12 and align with NIST guidelines and Governmentwide ICAM requirements; such as mobile and cloud identity.
 - (8) All USDA Mission Areas, agencies, and staff offices must follow the standard PIV exemption process approved by the ICAM Program Office and ISC.
 - (9) All USDA Mission Areas, agencies, and staff offices must require and implement the use of the PIV credential digital signature capability for internal business. For external business signature transactions, it is the responsibility of the USDA Mission Areas, agencies, and staff offices to use alternative digital or electronic signature mechanisms in compliance with NIST 800-63-3.
 - (10) All USDA Mission Areas, agencies, and staff offices; must ensure use of the PIV credential for physical access to Federal facilities and secured areas is implemented per the following:
 - (a) Cybersecurity & Infrastructure Security Agency (CISA) [*The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*](#), or any successive version.
 - (b) NIST [*SP 800-116*](#), Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access*, or any successive version.
 - (11) All USDA Mission Areas, agencies, and staff offices must update their technology roadmaps to adhere to the requirements of this policy.
- c. Acquisition of ICAM Capabilities and Services.
- (1) IT products and tools procured that require user authentication must comply with one of the following:
 - (a) Support PIV or other HSPD-12 compliant credentials; or
 - (b) Integrate with ICAM shared services that enable HSPD-12 compliant authentication through commercially available open standards.
 - (2) All contracts requiring contractors to have access to federally controlled facilities, or information systems, must include requirement to comply with HSPD-12 and FIPS PUB 201-2. This is based on OPM requirements and the *Federal Acquisition Regulation (FAR)*, [*48 Code of Federal Regulations \(CFR\) § 4.13*](#), *Personal Identity Verification*.

- (3) The Department of Homeland Security (DHS) CDM Program must be leveraged to accelerate procurement and deployment; of tools related to the ICAM capabilities of CDM.
- (4) Products and services acquired to further HSPD-12; and ICAM implementations; must be compliant with the following.
 - (a) OMB policy;
 - (b) NIST standards; and
 - (c) General Services Administration (GSA) [Approved Products List](#) (APL) and [CDM Approved Products List](#) (when applicable).

6. ROLES AND RESPONSIBILITIES

- a. The USDA Deputy Secretary, serving as the USDA Chief Operating Officer (COO), will:
 - (1) Ensure regular coordination among the CIO and USDA Mission Area, agency, and staff office leaders, to implement, manage, and maintain the USDA's ICAM policies, processes, and technologies; and
 - (2) Ensure establishment of an ICAM Advisory Council; that will maintain the charter for management of ICAM.
- b. The USDA Assistant Secretary for Administration will:
 - (1) Ensure USDA administrative programs, policies, advice, and counsel meet the needs of USDA programs and organizations consistent with laws and mandates;
 - (2) Provide safe efficient facilities and services to customers; and
 - (3) Sponsor the ICAM Advisory Council that will be established by the ICAM program.
- c. The USDA CIO will:
 - (1) Ensure the coordination, implementation, and management of all the Federal ICAM requirements;
 - (2) Designate the enterprise ICAM Program Office to manage and administer the USDA ICAM program; in accordance with the Federal governmentwide policies and regulations;

- (3) Designate the solutions for the ICAM services as the authoritative source; that encompass the entire USDA enterprise;
- (4) Provide oversight of the Mission Area, agency, and staff office acquisition of the ICAM technology solutions to eliminate duplication with enterprise shared service capabilities;
- (5) Provide oversight to promote and ensure the Mission Area, agency, and staff office compliance with this policy and associated DMs;
- (6) Define the ICAM related performance expectations for Mission Area Assistant CIOs, to support governmentwide management requirements such as PMA CAP goals; and
- (7) Incorporate objectives for continual improvement of ICAM into USDA IT strategic plans and review with OMB, per [Circular A-11](#), *Preparation, Submission and Execution of the Budget*.

d. The USDA CISO will:

- (1) Provide oversight to the assessment and authorization of Mission Area, agency, and staff office systems to ensure compliance with this policy and associated DMs;
- (2) Incorporate Digital Identity Risk Management assessment, as outlined in NIST SP 800-63, into the existing NIST [SP 800-37 Revision 2](#), *Risk Management Framework [RMF] for Information Systems and Organizations* process, including the selection of assurance levels commensurate with the risk to systems and applications;
- (3) Ensure continued coordination between the USDA CDM Program and the USDA ICAM Program; and
- (4) Designate a representative to participate in the ICAM Advisory Council.

e. The USDA ICAM Program Manager will:

- (1) Provide ICAM shared service platforms to support managing identities and credentials, and access to USDA and Mission Area, agency, and staff office applications, systems, and services per Federal ICAM Architecture and CDM requirements;
- (2) Publish and maintain the ICAM DMs, guidance, or handbooks which will provide detailed information and guidance about the use of systems and processes to meet the requirements in this ICAM policy;

- (3) Operate enterprise ICAM systems in compliance with USDA security requirements; and be responsible for assessment, authorization and continuous monitoring for ICAM Shared Services;
 - (4) Establish and maintain an ICAM Advisory Council, including governance structure, functions, roles, and responsibilities that will be described in the ICAM Advisory Council Charter; and
 - (5) Establish and maintain an ICAM CAWG including governance structure, functions, roles and responsibilities; that will be described in the ICAM CAWG Charter. The ICAM CAWG will plan, coordinate, and implement Mission Area, agency, and staff office specific ICAM initiatives, directives and activities; in coordination with the ICAM Program Office and communicate processes and procedures to its user population.
- f. The Chief Security Director, OSSP, will:
- (1) Designate a representative and alternate to participate in the ICAM Advisory Council;
 - (2) Offer consultation services in ICAM program, policy, and process direction for homeland security and emergency coordination activities and responsibilities;
 - (3) Maintain an enterprise Physical Access Control Systems (ePACS) capability and assist and support to integrate it with enterprise ICAM shared services; and
- g. The Deputy Director, OHRM will:
- (1) Designate a representative to participate in the ICAM Advisory Council;
 - (2) Develop and issue USDA wide policies and procedures to ensure that OHRM, Mission Area, agency, staff office, or external services that process new employees, accurately and timely enter all identity information required for ICAM compliance so that identity data for new hires is available to the ICAM system before their start date;
 - (3) Maintain 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 through guidance from the ICAM Advisory Council;
 - (4) Collaborate with the USDA ICAM Program Office to identify attributes in human resource 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; and

- (5) Develop policies and procedures to ensure that access to Departmental information systems is granted only to individuals with an established need to know and meeting the minimum interim or full background investigation requirements consistent with the information system and level of access; being requested.
- h. USDA Mission Area Assistant CIOs will:
- (1) Comply with this policy, associated DMs, and ICAM related mandates, regulations, and guidance;
 - (2) Designate a Mission Area ICAM Liaison to coordinate activities with the USDA ICAM Program Office and to participate in the Advisory Council;
 - (3) Ensure compatibility of Mission Area, agency, and staff office Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS) with Departmental systems, policies, and procedures;
 - (4) Use enterprise ICAM shared services for the creation, maintenance, and removal of identity and credential information for all persons accessing USDA PACS and LACS;
 - (5) Ensure that all persons accessing Departmental systems have a USDA accepted identity;
 - (6) Enforce the PIV card usage to meet Federal requirements;
 - (7) Ensure all relevant attributes have been appropriately completed;
 - (8) Request extensions or exceptions per Departmental guidance for systems or processes that cannot be aligned to the ICAM program directives;
 - (9) Waivers or request for deviations of the approved ICAM program requirements are still required to meet all Federal ICAM requirements; and
 - (10) Work with the USDA ICAM Program Office and USDA CDM Program to understand requirements and identify future CDM phase capabilities that support ICAM goals.
- i. The Senior Mission Area Officials Responsible for administrative business operations will:
- (1) Establish standardized roles and responsibilities to process onboarding and separation actions for all USDA personnel;
 - (2) Identify the responsible party or organization to process onboarding and separation actions for all USDA non-federal personnel;

- (3) Ensure processing of onboarding and separation actions for all USDA non-federal personnel is completed in USDA's enterprise Human Resources authoritative system for non-federal personnel; and
 - (4) Ensure policies and procedures are established to process and enter:
 - (a) New actions for all USDA personnel into designated USDA enterprise identity systems; prior to entry on duty date; and
 - (b) Separation actions for all USDA personnel into USDA enterprise systems prior to the personnel's separation date.
- j. The Mission Area Human Resources Directors (MAHRD) will:
 - (1) Implement procedures to process and enter:
 - (a) New actions for USDA employees into USDA enterprise systems prior to entry on duty date; and
 - (b) Separation actions for USDA employees into USDA enterprise systems; in advance of employees' separation date.
- k. Mission Area ICAM Liaisons will:
 - (1) Support and participate in the ICAM Advisory Council;
 - (2) Work directly with the ICAM Program Office on all ICAM program activities;
 - (3) Assist the USDA CIO with implementing ICAM in the Department and provide all details when any service or systems will be integrated; or removed from the USDA ICAM system;
 - (4) Serve as the primary coordinator for all ICAM related activities in the Department and prioritize ICAM implementations as directed by USDA leadership organizational leadership, and business needs; and
 - (5) Provide reports and data on the USDA Agency ICAM implementation activities and progress as requested by the ICAM Program Office, or as required by Federal directive.
- l. USDA personnel will:
 - (1) Notify their PIV credential sponsor or human resources point of contact of any changes in identity information, such as legal name or citizenship status;

- (2) Use their PIV or other HSPD-12 compliant credential for accessing information systems and facilities and follow the set procedures when PIV enforcement is not available;
- (3) Use only the USDA approved credential(s) for accessing PACS and LACS in USDA;
- (4) Not share their credentials or secret keys with another person;
- (5) Secure their credentials and secret keys in a way that reduces the likelihood that others will use them; and
- (6) Return their PIV or other HSPD-12 compliant credential for accessing information systems and facilities when separating from USDA as an employee, contractor, intern or volunteer.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

- a. [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16 sets forth USDA policy, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunications equipment. DR 4070-735-001, Section 21, states that a violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action; and
- b. Such disciplinary or adverse action will be affected in accordance with applicable law and regulations, such as OPM and OMB regulations, and [5 CFR § 2635](#), *Standards of Ethical Conduct for Federal Employees of the Executive Branch*.

8. POLICY EXCEPTIONS

- a. All USDA Mission Areas, agencies, and staff offices; are required to conform to this policy. If a policy requirement cannot be met as explicitly stated, a waiver may be requested. To request the waiver to this policy the application system owner must follow the standard information security exception processes. Note that an approved waiver does not constitute compliance with policy. Policy waiver requests are further described below.
 - (1) Acknowledge non-compliance with policy and that an acceptable plan to remediate the weakness has been, or will be, implemented.
 - (2) Must be documented as indicated in USDA's [CAPE-SOP-003](#), *Plan of Action and Milestones (POA&M) Management Standard Operating Procedure*.

- b. Policy waiver request memoranda will be addressed to the USDA ICAM Director and submitted to ICAM.Services@usda.gov for review and decision. Unless otherwise specified, policy waivers are approved for one year and must be reviewed and renewed every fiscal year.
- c. To be considered for a waiver, an application system must meet the following requirements:
 - (1) A technical constraint that inhibits the use of, or integration with, the USDA enterprise ICAM services.
 - (2) A transition plan is provided detailing when the asset will be retired or integrated with the USDA enterprise ICAM service.
 - (3) Alternative solutions must adhere to the Federal ICAM Architecture, NIST regulations for digital identity including NIST SP 800-63-3, and CDM requirements. This information must be documented in the waiver.

9. INQUIRIES

All inquiries pertaining to the contents of this DR can be submitted to icam.services@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
APL	Approved Products List
CAO	Chief Acquisition Officer
CAP	Cross Agency Priority
CAWG	Cross Agency Working Group
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COO	Chief Operating Officer
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
DSS	Digital Signature Standard
EIMS	Enterprise Identity Management Services
ePACS	Enterprise Physical Access Controls System
FAL	Federation Assurance Level
FAR	Federal Acquisition Regulation
FICAM	Federal Identity Credential Access Management
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
IoT	Internet of Things
ISA	Interconnection Security Agreement
ISC	Information Security Center
IT	Information Technology
LACS	Logical Access Control System
MAHRD	Mission Area Human Resources Director
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OCIO	Office of the Chief Information Officer
OGC	Office of the General Council

OHRM	Office of Human Resource Management
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSSP	Office of Safety, Security, and Protection
PACS	Physical Access Control System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	PIV Interoperable Credential
PIV-D	Derived PIV Credential
PKI	Public Key Infrastructure
PMA	President's Management Agenda
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
RPA	Robotic Process Automation
SAOP	Senior Agency Official for Privacy
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Credential. An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a subscriber. Credentials can be something a person knows (such as password or personal identification number), something they have (such as a LincPass), something they are (such as a biometric feature) or some combination of these items. (Sources: [DM 4620-002](#), *Common Identification Standards for U.S. Department of Agriculture and Federal Identity, Credential, and Access Management 4 (FICAM) Roadmap and Implementation Guidance*, December 2, 2011)

Derived PIV credential (PIV-D). A credential issued based on proof of possession and control of a PIV smart card that has been issued in accordance with FIPS PUB 201-2. When applied to PIV, identity proofing, and vetting processes do not have to be repeated to issue a Derived PIV Credential. (Sources: NIST, [FIPS PUB 201-2](#), *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

Governance. A set of processes that ensures the effective and efficient use of information technology in enabling an organization to achieve its goals. (Source: [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*)

Non-Person Entity (NPE). Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object. (Source: *Federal Identity, Credential, and Access Management 4 (FICAM) Roadmap and Implementation Guidance*, December 2, 2011)

PIV credential. PIV smart cards or other form factors that comply with FIPS 201-2 or superseding standards. This includes technological enhancements of LincPass Smart Cards and derived credentials. (Source: NIST, [FIPS PUB 201-2](#), *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

PIV-I credential. PIV interoperable smart card that complies with FIPS 201-2 or superseding standards. (Source: NIST, FIPS PUB 201-2, *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

Sponsor. The Sponsor is the employer or agency official responsible for authorizing and individual to apply for a credential, who has undergone Sponsor training and is designated to perform Sponsor functions. In the case of a contractor employees, the Sponsor maybe e the Contracting Officer's Representative (COR), Contracting Officer's Technical Representative (COTR), or another designated program official. (Source: DM-4620-002, *Common Identification Standards for U.S. Department of Agriculture*).

APPENDIX C

AUTHORITIES AND REFERENCES

Committee on National Security Systems (CNSS), [CNSS Directives](#) web page

CNSS, [CNSS Instructions](#) web page

CNSS, [CNSS Policies](#) web page

CNSS, [CNSS Standards](#) web page

Department of Homeland Security (DHS), [Cybersecurity & Infrastructure Security Agency \(CISA\), Continuous Diagnostics and Mitigation \(CDM\)](#) web site

DHS, CISA, Interagency Security Committee, [The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard](#), 2nd Edition, November 2016

DHS, [Homeland Security Presidential Directive \(HSPD\) 12](#), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

The Electronic Communications Privacy Act of 1986, [18 United States Code \(U.S.C.\) § 2701 et seq.](#), October 21, 1986

The Electronic Signatures in Global and National Commerce Act, [Public Law 106-229](#), June 30, 2000

Federal Acquisition Regulation (FAR), [48 CFR § 4.13](#) *Personal Identity Verification*

[Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance, Version 2.0](#), December 2, 2011

Federal Information Security Modernization Act (FISMA), [44 U.S.C. § 3551 et seq.](#), December 18, 2014

GSA, [Continuous Diagnostics & Mitigation \(CDM\) Program - Approved Products List](#) web site

Government Paperwork Elimination Act, [44 U.S.C § 3501 et seq.](#), October 21, 1998

NIST, [FIPS PUB 186-4](#), *Digital Signature Standard (DSS)*, September 2013

NIST, [FIPS PUB 201-2](#), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013

NIST, [SP 800-37-2](#), *Risk Management Framework for Information Systems and Organizations*, December 2018

NIST, [SP 800-47](#), *Security Guide for Interconnecting Information Technology Systems*, August 2002

NIST, [SP 800-53-5](#), *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020 with updates as of December 10, 2020

NIST, [SP 800 63-3](#), *Digital Identity Guidelines*, December 2017

NIST, [SP 800-116](#), Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access*, June 2018

NIST, [SP 800-157](#), *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014

Office of Government Ethics, *Standards of Ethical Conduct for Federal Employees of the Executive Branch*, [5 CFR § 2635](#), et seq.

OMB, Circular [A-11](#), *Preparation, Submission and Execution of the Budget*, July 10, 2020, as amended

OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*, July 28, 2016

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 [M-06-21](#), *Reciprocal Recognition of Existing Personnel Security Clearances*, July 17, 2006

OMB, Memorandum [M-19-17](#), *Enabling Mission Delivery through Improved Identity, Credential and Access Management*, May 21, 2019

OMB, Memorandum, [Reciprocal Recognition of Existing Personnel Security Clearances](#), December 12, 2005

President's Management Agenda (PMA) Cross Agency Priority (CAP) goals

The Privacy Act of 1974, [5 U.S.C. § 552a](#), December 31, 1974

USDA, [CAPE-SOP-003](#), Revision 1.1, *Plan of Action and Milestones Management Standard Operating Procedure*, November 2015

USDA, *CAWG Charter*

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

USDA, DM 3640-xxx, *Identity, Credential, and Access Management Procedures*, forthcoming

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

USDA, [DR 0100-001](#), *Departmental Directives System*, January 4, 2018

USDA, [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, April 20, 2021

USDA, [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 4, 2007

USDA, [DR 4620-002](#), *Common Identification Standard for U.S. Department of Agriculture*, March 22, 2021

USDA, [DR 4720-001](#), *USDA Onboarding Requirements*, June 3, 2011

USDA, ICAM Advisory Council Charter

USDA, [ICAM Service Catalog](#) web page