ADS 542

Identity, Credential, and Access Management (ICAM)

New Edition Date: 10/30/2020
Responsible Office: M/CIO/IPM
File Name: 542_103020

Functional Series 500 – Management Services
ADS 542 – Identity, Credential, and Access Management (ICAM)
POC for ADS 542: Sankar Das, (202) 916-2465, sadas@usaid.gov

This is a new ADS chapter.

Table of Contents

542.1 OVERVIEW

Effective Date: 10/30/2020

The United States Agency for International Development (USAID) must be able to identify, credential, monitor, and manage individuals that access Federal resources to promote secure and efficient operations. Federal resources include information, information systems, facilities, and secured areas across the Agency. To safeguard our Federal resources, USAID conducts identity proofing under **Federal Information Processing Standards (FIPS) Publication 201-2, Personal Identity Verification of Federal Employees and Contractors** and **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identity Guidelines** to establish enterprise digital identities, and has adopted processes for authentication and access control to ensure the security and delivery of Agency services, as well as individuals' privacy.

USAID has established Identity, Credential, and Access Management (ICAM) governance as an important part of its continual efforts to promote robust cybersecurity. The Agency leverages the approaches and principles contained in **Office of Management and Budget (OMB) Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management**, while continuing to follow requirements in **Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors**, pertaining to the identity verification and credentialing of Federal employees and contractors.

This ADS chapter outlines Federal Government-wide ICAM responsibilities and requirements in areas such as multi-factor authentication, encryption, digital signatures, acquisition, and interoperability. Additionally, USAID identity proofing processes are addressed in this chapter. USAID validates, manages, and controls all identities (both users and information technology (IT) devices) on the network with a uniform trusted certificate lifecycle process that meets Federal guidelines. Members of the USAID workforce receive credentials as part of the on-boarding process which are revoked as part of the off-boarding process. USAID IT devices are issued certificates using an identity process unique to each certificate type that includes validation by the system owner.

This policy applies to the USAID workforce (see applicability statement in the next paragraph) and IT equipment, workstations, systems, information, and services, owned by or operated on behalf of USAID. It is designed to protect the Agency’s IT assets and information from unauthorized access, use, disclosure, disruption, modification, and/or destruction.

Throughout this chapter, the terms "workforce" and “users” refer to individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement (PASA) and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS Chapter 501, The Automated Directives System**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and Information Security requirements.

542.2 PRIMARY RESPONSIBILITIES

Effective Date: 10/30/2020

a. The **Deputy Administrator, as the Agency Chief Operating Officer (COO)**, co-chairs the Management Operations Council (MOC) which is the oversight body for the Information Technology Steering Subcommittee (ITSS) and performs their validation/clearance role to enterprise-level ICAM that require clearance (*e.g.*, changes that impact Agency-wide processes).

b. The **Chief Information Officer (CIO)** is responsible for implementing an Agency-wide ICAM architecture that includes people, processes, and technology. The CIO serves as the permanent chair of the ITSS.

c. The **Chief Information Security Officer (CISO)** is the Agency's senior information security official. The CISO carries out CIO security responsibilities under the Federal Information Security Modernization Act (FISMA) and Risk Executive functions for the Agency. The CISO is a permanent member of the ITSS.

d. The **Bureau for Management, Office of the Chief Information Officer, Information and Process Management Division (M/CIO/IPM)** oversees the daily functions of the ICAM Program. The ICAM Program is responsible for developing, maintaining, and updating the Agency ICAM policies and processes as well as providing USAID with the architecture, capabilities, and tools required to prioritize risk management and enable cybersecurity tactics that will mitigate significant problems. Under the direction of M/CIO/IPM, the ICAM Program provides technical support to the ITSS to ensure the Agency's ICAM policies, processes, and technologies are implemented, maintained, and managed consistently with **OMB M-19-17**.

The M/CIO/IPM is an official designee on the Federal ICAM Subcommittee (SC) and has overall responsibility for providing technical guidance to the USAID ICAM Governance Board apprised of all ICAM implementations spanning across the enterprise for logical security.

e. The **Office of Security (SEC)** is an official designee to the Federal ICAM Subcommittee (SC) and has responsibility for providing technical guidance to the USAID ICAM Governance Board of all ICAM implementations spanning across the enterprise for physical security.

f. The **Senior Agency Official for Privacy (SAOP), in the Bureau for Management**, has responsibility and accountability for implementing Agency privacy policy and protections, including USAID's compliance with Federal laws, regulations, and policies relating to privacy. The SAOP is a permanent member of the ITSS.

g. The **Chief Acquisition Officer (CAO), in the Bureau for Management**, manages and directs the Agency's Acquisition and Assistance system and commodity transportation and is a permanent member of the ITSS.

h. The **Chief Human Capital Officer (CHCO), in the Office of Human Capital and Talent Management (HCTM)**, serves as USAID’s chief policy advisor on all human resource management issues and is a permanent member of the ITSS.

i. The **Chief Financial Officer (CFO), in the Bureau for Management**, directs USAID financial management operations worldwide and is a permanent member of the ITSS.

j. The **Director, Office of Security (SEC)**, supervises, directs, and controls all security activities relating to the programs and operations of USAID, except for unclassified automated security systems, and is a permanent member of the ITSS.

k. The **Office of the General Counsel (GC)** provides legal advice, counsel, and services to the Agency and its officials, ensures that USAID programs are administered in accordance with legislative authorities, and is a permanent member of the ITSS.

l. The **Information Technology Steering Subcommittee (ITSS) of the Management Operations Committee (MOC)** is sponsored by the CIO and is the Agency-wide executive IT investment governance body that ensures that the Agency’s ICAM policies, processes, and technologies are being implemented, maintained, and managed consistently with **OMB M-19-17**. The ITSS serves as the Agency ICAM Governance Board.

m. The **System Owner (SO)** is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for addressing the operational interests of the user community (*i.e.,* users who require access to the information system to satisfy Mission, business, or Agency requirements) and for ensuring compliance with ICAM requirements (*e.g.,* business, technical, security, and risk).

n. The **Business Owner (BO)** is responsible for funding and other resources that support their line of business to ensure ICAM requirements are implemented and sustained.

542.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 10/30/2020

This chapter sets forth the ICAM policy guidance for USAID. Implementation of ICAM strengthens the security of information and information systems in the Agency by applying security requirements that allow the Agency to enable the right identities (*e.g.,* users) to access the right resources at the right time for the right reasons. For the purposes of this chapter, ICAM is the combination of technical systems, policies, and processes that create, define, and govern the use and safeguarding of identity information by bonding digital identities to “user” and “device” identities, as well as managing the relationship between an entity and the resources to which access is needed.

These principles work together to authenticate the identities, privileges, and roles of all USAID workforce members, which helps determine if an individual should have access to specific USAID facilities or information systems. The Agency’s ICAM Program enterprise solution manages access control policies and provides automated provisioning, management, and de-provisioning of identities and physical and logical access entitlements across USAID facilities, the enterprise, and Agency IT systems.

USAID’s adoption of ICAM requirements includes the:

1) Implementation of effective governance,

2) Modernization of Agency capabilities, and

3) Agency adoption of shared solutions and services.

In accordance with **OMB M-19-17**, USAID has implemented an enterprise risk management plan, which includes selecting the appropriate digital identity services, assurance levels, and credentials per data classification. USAID’s enterprise risk management plan is aligned with **NIST SP 800-37, Risk Management Framework**.

USAID must enforce ICAM strategies and solutions that implement **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3** and the **Risk Management Framework**.

USAID must implement **NIST SP 800-63-3** to set the foundation for identity management and its usage to access physical and digital resources. **OMB M-19-17** enforces that **NIST SP 800-63** is the foundation for digital identity; agencies must use it in combination with the remaining suite of publications that relate to identity management issued by NIST, the Office of Personnel Management (OPM), and the Department of Homeland Security (DHS).

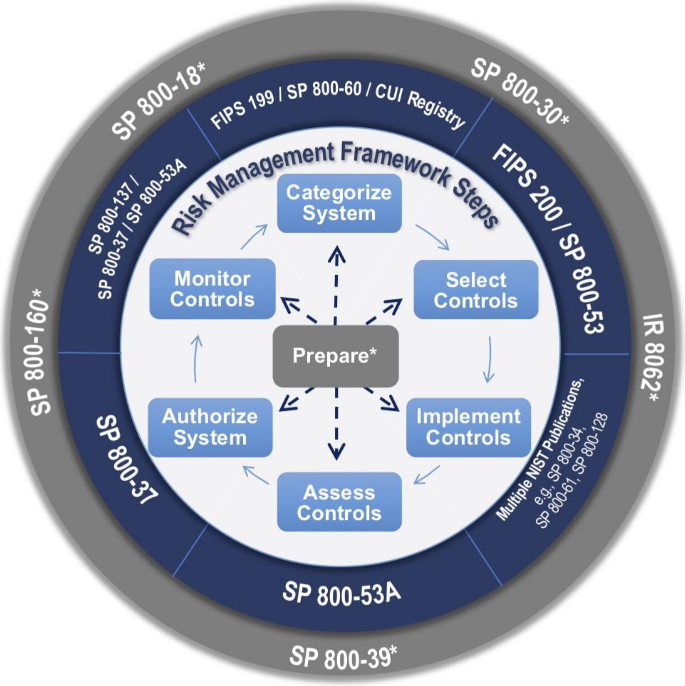

Figure 1: Risk Management Framework

The above graphic (Figure 1) represents the NIST Cybersecurity Framework, showing the interconnections between multiple NIST Special Publications and the FIPs guidelines.

The USAID Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle.

For additional information on the Agency Risk Management Plan, contact **ato@usaid.gov**.

542.3.1 ICAM Program Governance

Effective Date: 10/30/2020

The USAID ICAM program implements Federal policy and mandates from OMB, the Department of Homeland Security (DHS) on Continuous Diagnostics and Monitoring (CDM), and Federal ICAM and Public Key Infrastructure (PKI) directives.

M/CIO and SEC are USAID’s official designees on the Federal ICAM Subcommittee (ICAMSC) which is the interagency forum for identity management, secure access, authentication, authorization, credentials, privileges, and access lifecycle management.

M/CIO, in coordination with SEC, manages the Agency’s ICAM program. M/CIO oversees changes to the ICAM requirements or processes and reviews any changes with the ITSS on an annual basis unless emergency changes necessitate more frequent updates/reviews.

542.3.2 Identity Management

Effective Date: 10/30/2020

USAID must manage all identities by performing the identity verification as required in Identity Assurance Level components in **NIST 800-63-3**. The background adjudication will bind the identities to their digital identity assurance level. USAID must issue the appropriate credentials based on a users' digital identity assurance level (IAL) requirements and access control.

Before individuals are granted unescorted access to USAID/W government facilities as well as logical access to Agency networks, all requirements of HSPD-12 must be met. The requirements are as follows:

a. Favorable adjudication of clearance or background investigation;

b. Sponsorship by a USAID Direct-Hire (DH), U.S. Personal Services Contractor (USPSC), or other proper authority;

c. Completion of in-person enrollment/identity proofing. An employee or contractor is issued a credential only after presenting two identity source documents to the Enrollment Office, at least one of which must be a valid Federal or state government-issued picture identification (see **HSPD-12 and reference Form I-9, Employment Eligibility Verification**, for a complete list of acceptable documents as proof of identification); and

d. Attendance at a required M/CIO CISO/Privacy briefing and the SEC initial security briefing (Note: Individuals must submit the documentation provided at the training during enrollment).

Note: In limited scenarios, such as mandatory extended government-wide telework where the Agency has determined that in-person enrollment badge issuance and attendance at required Privacy and SEC initial security briefings are not practicable, new workforce members or detailed employees that have received an approved AID 565-1 may be eligible to receive logical access to Agency systems upon completion of virtual New Employee Orientation (NEO) training.

The B/IO AMS Officer must register the new workforce members for virtual NEO training once they have received an approved AID 565-1 from SEC. Once the 565-1 is SEC-approved, the M/CIO Enrollment Team will schedule a one-on-one Virtual Identity Proofing/Enrollment session with the individual. Once the virtual session has been completed the M/CIO Enrollment Team will initiate a request to finalize the individual's network account and assigns a temporary network password. The individual will be able to access the Agency network and email when they issued an RSA token. Once onsite work resumes, the individual may be required to undergo additional processes to complete the enrollment process.

Federal employees detailed from another agency, that have received a favorable adjudication and have a PIV from their home agency, are eligible for a Facility Logical Access Card (FLAC) to have unescorted physical and logical access to USAID facilities upon completion of SEC and M/CIO required Privacy and Security NEO training.

Individuals who are not eligible or do not require a Federal PIV card may be issued a FLAC for physical and logical access or a Facility Access Card (FAC) for physical access to USAID facilities. Applicants receiving a FLAC or FAC must undergo sponsorship, enrollment, and card issuance before any unescorted physical access to USAID facilities. FLAC and FAC do not meet the specifications of **FIPS 201** and must not be used as Federal identification cards.

Overseas staff who fall into the Cooperating Country National (CCN) PSC, Third Country National (TCN) PSC, or Foreign Service National (FSN) use case are issued USAID PIV-A cards after meeting the requirements of a National Agency Check (NAC).

542.3.3 Credential Management

Effective Date: 10/30/2020

USAID enforces the **Homeland Security Presidential Directive 12 (HSPD-12)** and **NIST 800-63-3, FIPS 201-2 Identity Vetting Requirements** for credentialing USAID user identities. Before identities can be credentialed, USAID Bureaus, Independent Offices and Missions (B/IO/Ms) must initiate the on-boarding process, based on the user type, to issue the correct credential.

HSPD-12 is the government-wide policy for the promulgation of standards-based, secure, and reliable forms of identification issued by the Federal Government to its employees, contractors, and other enterprise users. Additionally, **Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors** (or successive version) is the government-wide standard for common identification, as called for by **HSPD-12**.

This chapter incorporates guidance to include the Agency policy governing issuance, maintenance, and use of Agency-issued Federal identification credentials (PIV, FAC, and FLAC access control cards and their use in conjunction with the **Federal Information Processing Standards (FIPS) 201** initiative and the **HSPD-12** directive). For guidance on processes please see **ADS 565, Domestic Security Programs**.

This chapter also sets the policies for the issuance, maintenance, and use of the:

- **Federal Bridge PKI Certificate Policy** for the Agency's PIV-Alternative (PIV-A);

- **NIST SP 800-63-3** identity proofing through implementing Identity Assurance Level (IAL), Authentication or Assurance Level (AAL) 3, Federal Assurance Level (FAL) credentials into the Agency's technical architecture;

- **NIST Special Publication (SP) 1800-12, Derived Personal Identity Verification (PIV) Credentials**;

- **NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials**; and

- Approved products for smart authentication in accordance with **NIST SP 800-63-3 A**; Federal Identity assurance levels are included as well.

542.3.3.1 Issuing Credentials to USAID Workforce

Effective Date: 10/30/2020

USAID issues six various types of credentials to users who require physical access to Agency facilities and/or logical access to Agency information systems. This approach provides controlled access to USAID facilities and information technology resources. USAID also assigns credentials to user identities based on the Identity Requirements in the table below.

#	Credential Type	Identity Requirement	Credential Issuer	Identity Type
1	PIV	Investigation with NAC-I	State	U.S. Citizen/Federal Civilian/U.S. Contractor clearance
2	PIV-A	Investigation with NAC RSO/State	M/CIO	Foreign Service National, Cooperating Country National PSC (CCNPSC) and Third Country National PSC (TCNPSC)
3	Facility Logical Access Card (FLAC)	Investigation with NAC-I	State	Detailed employee from another agency that has their home agency PIV card and Interim clearances
4	Facility Access Card (FAC)	Investigation with NAC-I	State	Physical Access Only
5	Derived PIV Credential (DPC)	Investigation with NAC-I	M/CIO	U.S. Citizen/Federal Civilian/U.S. Contractor
6	PIV-A Derived Credential	Investigation with NAC	M/CIO	FSN/Detailed Employee from another agency that has their home agency PIV card

USAID must verify all identities in the Agency and credential users accordingly.

Although there are several identity proofing processes for USAID users, all internal identities are vetted to a National Agency Background Check (NAC) or National Agency Background Check with written Inquiries (NAC-I) for network logical and physical access. For guidance on obtaining a USAID credential please see **ADS 565**. For guidance on how to apply for a facility clearance for a member of the USAID workforce, see **ADS 566, Personnel Security Investigations and Clearances** and **ADS 567, Classified Contracts and Awards Under USAID's National Industrial Security Program**.

542.3.3.2 Obtaining a USAID/W Personal Identity Verification (PIV) Card, Facility Logical Access Card (FLAC)

Effective Date: 10/30/2020

Individual USAID Direct-Hires, USPSCs, contractor employees, and other government entities, including Congress, who require either physical or logical access for more than 15 business days must be sponsored by a USAID B/IO to obtain a Federal ID/PIV or FLAC.

To obtain the appropriate background adjudication and clearance for USAID Direct-Hires, USPSCs, and contractor employees on unclassified contracts, SEC requires the completion of **USAID Form AID 6-1 Request for Security Action**.

Other government entities, including Congress and those contractor employees on classified contracts must submit a **USAID Form 565-2** or Visit Authorization Letter (VAL) as applicable.

To obtain logical access to Agency networks, an individual must first receive a USAID Personal Identity Verification (PIV) card or FLAC. To initiate this process, the Administrative Management Services (AMS) Officer must submit a completed **USAID Form AID 565-1** to the Office of Security (SEC). SEC must issue a favorable adjudication for physical/network access to be granted.

See **542.3.2** for guidance on obtaining logical access in limited exceptional circumstances such as mandatory extended government-wide telework.

542.3.3.3 Obtaining an Outside Continental United States (OCONUS) Personal Identity Verification-Alternative (PIV-A) Card

Effective Date: 10/30/2020

The PIV-A credential is issued to USAID staff overseas who cannot be issued a PIV (HSPD-12 PIV credential) since they are not U.S. citizens. PIV-A credentials may be issued to overseas staff who have undergone a State Department NAC to be hired onto the USAID Network. This credential is strictly limited to Foreign Service Nationals, CCNPSCs, and TCNPSCs who require physical and/or logical access. These individuals must be vetted and cleared subscribers who have passed a National Agency Check (NAC) by the Department of State Regional Security Officer (DoS RSO) and have been issued a medium-hardware assurance credential to be eligible for a PIV-A credential.

The Local Registration Authority (LRA) (in OCONUS, the Mission Executive Officer (EXO) serves as the LRA) or Registration Authority (RA) must be a U.S. Citizen PIV cardholder to verify an FSN, CCNPSC, TCNPSC identity and NAC. The LRA/EXO must submit a request for a PIV-A card for each user via **Service Central** or **cio-helpdesk@usaid.gov**. Once the Department of State issues a NAC, the LRA issues the PIV-A with the credentials approved by M/CIO.

542.3.3.4 Derived PIV and PIV-Derived Credentials

Effective Date: 10/30/2020

USAID must implement mobility access controls that follow the Federal NIST **Special Publication (SP) 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials** and NIST SP 1800-12, Derived PIV Credentials. USAID derived credentials must meet NIST guidelines for issuance and lifecycle management ensuring that PIV credentials for users whose certificates have expired are not revoked outside the time allowed. USAID derived credentials must be revoked based on NIST requirements. These credentials leverage the trust of the bonding digital identity to enable USAID users to access resources from a mobile platform as well as act as the authenticator for USAID multi-factor authentication (MFA) users to access other federated services, such as the Office of Management and Budget **https://portal.max.gov/portal/home** site which validates whether the PIV/PIV-A user credential is still active.

542.3.3.5 Physical Access to USAID Facilities

Effective Date: 10/30/2020

In USAID/Washington (USAID/W), PIV, Facility Logical Access Cards (FLAC) and Facility Access Card (FAC) are issued to U.S. citizens and resident aliens that are members of the USAID workforce.

For Outside Continental United States (OCONUS) locations, physical access is controlled by the Department of State-issued Embassy badge.

For additional guidance on physical access to Agency facilities, see **ADS 565, Domestic Security Programs**.

542.3.3.6 Obtaining a USAID/W Facility Access Card (FAC)

Effective Date: 10/30/2020

USAID Direct-Hires, USPSCs, contractor employees and other government entities, including Congress, who require only physical access for more than 15 days must be sponsored by a USAID B/IO to obtain a USAID FAC.

To obtain the appropriate background adjudication and clearance for USAID Direct-Hires, USPSCs, and contractor employees on unclassified contracts, SEC requires the completion of **USAID Form AID 6-1 Request for Security Action for each employee requesting access**.

Other government entities, including Congress and those contractor employees on classified contracts must submit a **USAID Form 565-2** or Visit Authorization Letter (VAL), as applicable, for each individual requesting access.

To obtain only physical access to USAID facilities, an individual must first receive a USAID FAC. To initiate this process, the Administrative Management Services (AMS) Officer must submit a completed **USAID Form AID 565-1** to the Office of Security (SEC). SEC must issue a favorable adjudication for physical/network access to be granted (see **ADS 565, Domestic Security Programs** for additional guidance).

542.3.3.7 Public Key Infrastructure (PKI) Non-Person Entity Credentialing

Effective Date: 10/30/2020

USAID has implemented and enabled PKI that supports strong authentication compliant with OMB M-19-17 and the associated NIST and FIPS required standards. The Department of State and Federal Bridge Entrust PKIs must be enabled within USAID to use the required PIV cards issued and must validate user identity on the network before allowing access.

The USAID PKIs enable strong authentication and will act as authenticators to support all NIST 800-63-3 assurance level components (*e.g.,* Identity, Authentication and Federation). USAID mandates the process in which all PKIs that are deployed must not contradict mandatory and binding standards and guidelines for Federal agencies. The following section provides additional background on USAID’s implementation of PKI.

All devices in the Agency will be issued a USAID Non-Person Entity (NPE) identity certificate that uniquely identifies the devices on the network.

All system and application owners must use certificates for internal encryption to enable strong authentication as part of USAID encryption processes.

For public facing websites, M/CIO mandates compliance with OMB M-15-13, “A Policy to Require Secure Connections across Federal Websites and Web Services.” All USAID public facing websites must follow the same encryption requirements as internal systems and be enabled for transport.

The USAID NPE must maintain a set of trusted roles that ensure the PKI remains in the same state in which it was deployed. Trusted roles are required to complete annual training.

542.3.4 Encryption

Effective Date: 10/30/2020

M/CIO enforces agency-wide encryption requirements that meet FIPS 140-3, the mandatory standard for cryptographic-based security systems in computer and telecommunication systems (including voice systems), for the protection of all USAID information and information systems. Encryption is a critical security control for implementing ICAM. USAID complies with Federal encryption standards.

USAID also enforces the Agency's encryption standards for all cloud services. USAID's information and information systems are protected with services and tools to identify, monitor, and manage data in use, in transit, and at rest. Data protection policies are applied based on USAID requirements and business processes. See **ADS 508, Privacy Program**, **545, Information Systems Security**, and **ADS 545mbd, Rules of Behavior for Users** for Agency policy on encryption.

542.3.5 Digital Signature

Effective Date: 10/30/2020

Digital signatures are a type of electronic signature, and this policy requires the use of digital signatures to the greatest extent practicable. The term digital signature means a method of signing an electronic message and/or electronic document that: (A) identifies and authenticates a particular person as the signatory (B) indicates such person's approval of the information contained in the electronic message or document, and (C) prevents alteration of the signature (*e.g.,* non-repudiation).

As a policy matter, the Agency, to the greatest extent practicable, requires the use of a PIV or PIV-A card along with derived credentials for digital signatures (referred to as PIV throughout this section), in compliance with **OMB-A-130**, **NIST SP 800-63, Digital Identity Guidelines**, and **HSPD-12**. Members of the USAID workforce must use PIV cards when digitally signing official Agency documents as they become enabled to support digital signatures, unless an exception applies/to the greatest extent practicable (*e.g.,* exceptions such as PIV or PIV-A credentials have expired or there are technical limitations). The SO and/or BO are responsible for working with M/CIO to enable official Agency documents (*e.g.,* contracts, etc.) for digital signature and other ICAM digital identity requirements.

Use of PIV digital signature is the required method to the greatest extent practicable for all official and binding USAID documents that require a signature. A PIV card mitigates security vulnerabilities by providing authentication and ensuring the identity of the signer.

OMB M-19-17 and **NIST 800-63-3** requires that Agencies implement the use of the PIV credential digital signature capability. USAID requires the use of a digital signature for individuals that fall outside the scope of PIV applicability (*e.g.,* an unbadged individual).

542.3.6 Access

Effective Date: 10/30/2020

M/CIO must manage the Dynamic Access Controls (DAC) by automating account management approvals and processes for granting or removing access (*e.g.,* account management), as well as privileged entitlements.

542.3.6.1 Dynamic Access Control

Effective Date: 10/30/2020

All digital identities, entitlements, and privileges must be managed dynamically.

USAID leverages automated sources to report the identity and access control levels to the Department of Homeland Security Continuous Monitoring Federal dashboard. The USAID automation tools and Artificial Intelligence (AI), make the digital identities distinguishable, auditable, and consistently managed across the agency. This includes establishing mechanisms to bind, update, revoke, and destroy credentials for the user and/or device or automated technology.

M/CIO IT Operations (ITO) and M/CIO Information Assurance (IA) must monitor and review these identity access controls annually for accurate reporting.

USAID must ensure that deployed ICAM capabilities are interchangeable, use commercially available products, and leverage open Application Programming Interfaces (APIs) and commercial standards to enable development and promote interoperability across all levels of government.

542.3.7 Privileged Access Management

Effective Date: 10/30/2020

M/CIO must control and manage access to privileged accounts using an enterprise-wide solution enforcing strong authentication to all the organization's system interfaces.

M/CIO must review privileged account access annually to ensure that the privileged access is still required, and that the individual has successfully completed required annual security training. Privileged users must digitally sign and accept their role as a USAID elevated user on an annual basis (see **ADS 545.3.2.6 Least Privilege (AC-6)** for additional information).

542.3.8 Federation

Effective Date: 10/30/2020

USAID will leverage the Federal capabilities to collaborate with other agencies and partners. These types of collaborated services (*e.g.,* **https://portal.max.gov/portal/home**) are determined by the **NIST 800-63-C Guidelines for Federation Assurance Levels (FALs)**. FAL refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP). USAID assigns and enforces FALs based on systems security risk assessments.

M/CIO must ensure that deployed federated ICAM capabilities are interchangeable and leverage open Application Programming Interfaces (APIs) and standards to enable development and promote interoperability.

542.4 MANDATORY REFERENCES

542.4.1 External Mandatory References

Effective Date: 10/30/2020

a. **Executive Order 13681 Improving the Security of Consumer Financial Transactions**

b. **FIPS 140-2 Security Requirements for Cryptographic Modules**

c. **FIPS 199-Standards for Security Categorization of Federal Information and Information Systems**

d. **FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors**

e. **Homeland Security Presidential Directive 12 (HSPD-12) – Policy for a Common Identification Standard for Federal Employees and Contractors**

f. **NIST 800-53-4 Security and Privacy Controls for Federal Information Systems and Organizations**

g. **NIST 800-57 Recommendation for Key Management**

h. **NIST 800-175B Cryptographic Standards**

i. **NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials**

j. **NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**

k. **NIST SP 1800-18B, Privileged Account Management for the Financial Services Sector**

l. **OMB Circular A-130, "Personally Identifiable Information" means information that can be used to distinguish or trace an individual's identity**

m. **OMB M-05-05 Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services**

n. OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

o. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identity Guidelines

542.4.2 Internal Mandatory References

Effective Date: 10/30/2020

a. ADS 508, Privacy Program

b. ADS 545, Information Systems Security

c. ADS 565, Domestic Security Programs

d. AID 565-1 (Request for Federal Identification Card/Facility Access Card)

e. AID 565-2 (Participating Agency Certification of Candidate's Security Clearance and Duration of Assignment)

f. AID 6-1 Request for Security Action

542.5 ADDITIONAL HELP

Effective Date: 10/30/2020

a. USAID ICAM Program Page (this may only be accessed via the Agency intranet)

542.6 DEFINITIONS

Effective Date: 10/30/2020

See the ADS Glossary for all ADS terms and definitions.

Continuous Diagnostic Monitoring (CDM)
The program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. CDM provides agencies access to tools that support their continuous monitoring efforts. Cybersecurity & Infrastructure Security Agency (CISA) (**Chapter 542**)

Credential Management (*e.g.,* credentialing)
How an agency issues, manages, and revokes credentials bound to enterprise identities. (Federal ICAM Architecture) (**Chapter 542**)

Cryptography

A method of protecting information and communications using codes so that only those for whom the information is intended can read and process it. (**FIPS 140-3 Cryptographic Standards**) (**Chapter 542**)

Device Identity
A USAID device and/or machine managed and credentialed identity by USAID. (**FPKI**) (**Chapter 542**)

Dynamic Access Controls
Domain-based controls that enable administrators to apply access-control permissions and restrictions based on well-defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration of the device that is used to access these resources. (**FISMA Metrics (October 2019)**) (**Chapter 542**)

Federal Enterprise Identity/Enterprise Identity
The unique representation of an employee, a contractor, an enterprise user, such as a mission or business partner, a device, or a technology that a Federal agency manages to achieve its mission and business objectives. (**NIST SP 800-63-3**) (**Chapter 542**)

Hardware Security Module
A physical computing device that safeguards and manages digital keys for strong authentication and provides crypto-processing. (**FIPS 140-3 Cryptographic Standards**) (**Chapter 542**)

Identity
The unique representation of a subject — for example, a person, a device, a non-person entity (NPE), or an automated technology - that is engaged in a transaction involving at least one Federal subject or a Federal resource, for example, Federal information, a Federal information system, or a Federal facility or secured area (**OMB M-19-17**). (**Chapter 542**)

Identity, Credential, and Access Management (ICAM)
The Federal Government Identity and Credential Access Management that dictates the requirements for Federal agencies to implement identity and access management. (**OMB M-19-17**) (**Chapter 542**)

Non-Person Entity (NPE) PKI
Enables users and systems to securely exchange data over the Internet and verify the legitimacy of certificate-holding entities, such as web servers, other authenticated servers, and individuals. (**CNSSI 4009-2015**, **DHS OIG 11-121**) (**Chapter 542**)

PKI Certificate
A public key used for encryption and cryptographic authentication of data sent to or from the entity that was issued the certificate. Other information included in a PKI certificate includes identifying information about the certificate holder, about the PKI that issued the certificate, and other data, including the certificate's creation date and validity

period. The PKI is the foundation that enables the use of technologies, such as digital signatures and encryption, across large user populations. PKIs deliver the elements essential for a secure and trusted business environment for e-commerce and the growing Internet of Things (IoT). (**https://www.idmanagement.gov/topics/fpki/**) (**Chapter 542**)

Public Key Infrastructure (PKI)
The set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys. (**Chapter 542**)

Trusted Roles
They are individuals with responsibilities and tasks assigned to trusted roles who implement "separation of duties" based on the security-related concerns of the functions to be performed. A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Please refer to Sections 1.3 and 5.2 in the **Federal Common Policy Framework**. (**Chapter 542**)

User Identity
USAID privileged user identities managed and credentialed by USAID NIST Identity Assurance Level (IAL), Assurance Level (AAL), Federal Assurance Levels (FAL), Common Policy X.509 Med Hardware Assurance Level, and NIST 800-157 PIV Derived Credentials (DPC). (**Chapter 542**)

542_103020