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: 09/27/2021

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 SP 800-157 guidelines for issuance and lifecycle management. PIV-derived credentials are continuously monitored on Certificate Revocation Lists (CRLs), ensuring that USAID is compliant with NIST 800-157 guidelines. The credentials are derived from the trust associated with the issued PIV credential and bond the digital identity to enable USAID users to access resources from a mobile platform.

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: 09/27/2021

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 intent to sign the electronic message or document, and (C) prevents alteration of the signature digital signatures are required to the greatest extent practicable by USAID because of their efficiency and effectiveness, including mitigating risks of non-repudiation (*e.g.,* signature alteration).

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, to the greatest extent practicable, unless an exception applies (*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.

PIV digital signatures must be used, 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** require that Agencies implement the use of the PIV credential digital signature capability. USAID requires – to the greatest extent practicable - 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: 09/27/2021

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

b. Executive Order 14028, Improving the Nation's Cybersecurity

c. FIPS 140-2 Security Requirements for Cryptographic Modules

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

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

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

g. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

h. NIST SP 800-57 Recommendation for Key Management

i. NIST SP 800-175B Cryptographic Standards

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

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

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

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

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

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

p. **OMB M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act**

q. **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: 09/27/2021

See the **ADS Glossary** for all ADS terms and definitions.

Certificate Revocation List (CRL)
A list of digital certificates revoked by the issuing certificate authority (CA) before their expiration date. (**Chapter 542**)

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_092721