

Approved: 2-19-2013
Chg 1 (LtdChg): 9-2-2022
Chg 2 (LtdChg): 10-28-2024

SUBJECT: IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

1. **PURPOSE.** To establish requirements and responsibilities for DOE's identity, credential, and access management program that:
 - a. Provides a trusted framework and common identity infrastructure for access to DOE facilities and systems;
 - b. Reduces the identity, credential, and access management burden for individual DOE and contractor organizations by fostering common interoperable approaches;
 - c. Aligns identity, credential, and access management activities that cross organizational boundaries;
 - d. Enables trust in online transactions through common identity, credential, and access management policies and approaches;
 - e. Establishes roles to enhance interoperability when collaborating with external identity management activities; and
 - f. Establishes the credentialing requirements for federal and contractor employees of the Department.
2. **CANCELLATION.** DOE O 206.2, *Identity, Credential, and Access Management (ICAM)*, dated 2-19-13. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.
3. **APPLICABILITY.**
 - a. **Departmental Applicability.** Except for the equivalencies/exemptions in paragraph 3.c., this Order applies to all DOE Elements.

The Administrator of the National Nuclear Security Administration (NNSA) must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

b. DOE Contractors.

- (1) Except for the exemptions in paragraph 3.c., the Contractor Requirements Document (CRD) sets forth requirements of this Order that will apply to contracts that include the CRD.
- (2) The CRD, or its requirements, must be included in contracts when:
 - (a) Contractor employees require routine access to a DOE facility or DOE information system; or
 - (b) The contractor operates a DOE facility or DOE information system.

c. Equivalency/Exemption.

- (1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
- (2) Exemption. DOE information systems that are considered “national security systems” as defined by 44 U.S.C. 3542(b)(2) are exempt from this Order.

4. REQUIREMENTS.

a. General.

- (1) DOE facilities and DOE information systems must meet the requirements of Office of Management and Budget (OMB)M-19-17, which requires that agency implementations align with the Federal Chief Information Officers Council’s *Federal Identity Credential Access Management (FICAM) Roadmap and Implementation Guidance*, and the FICAM Architecture and Continuous Diagnostics and Mitigation (CDM).
- (2) DOE must procure services and products that comply with HSPD-12 requirements in current Federal Acquisition Regulations and, where applicable, are on the General Services Administration (GSA) Approved Products List.

b. Identity.

- (1) Enterprise Identity Management Service. An enterprise identity management service (EIMS) must be developed and offered as a Department-wide service that:

- (a) Links authoritative sources of identity information on DOE employees and contractor employees;
 - (b) Establishes a unique identity record for each DOE employee and contractor employee;
 - (c) Provides DOE Elements a singular authoritative source for identity information to conduct DOE business; and
 - (d) Supports the management of federated identity records from trusted identity providers both internal and external to the Federal Government.
- (2) DOE Unique Identifier. All DOE employees and contractor employees must have a DOE unique identifier that remains with the individual forever. The DOE unique identifier must never be assigned to another individual. Individuals must always have the same DOE unique identifier:
 - (a) No matter how often they join and separate from DOE;
 - (b) If they move to/and from Federal employee or contractor employee status; or
 - (c) If they are employed by multiple contractors.
- (3) Identity Information. Information about an individual's identity should be collected only once and maintained in an authoritative data source and must be shared across DOE Elements through the EIMS.
- (4) Identity Record. The identity record in the EIMS must contain a DOE unique identifier and all identity information that is associated with DOE employee or contractor employee.
- (5) Authoritative Data Sources. Multiple authoritative data sources may contain information that constitute an identity record for an individual.
 - (a) A registry of authoritative data sources must exist and be maintained.
 - (b) Authoritative data sources must make available identity information to the EIMS.
 - (c) A responsible entity must be identified to maintain each authoritative data source.
- (6) Lifecycle Management. Identity information must be established and maintained by the DOE entity which is responsible for the accuracy of the information. The DOE unique identifier ensures that an individual only has one identity record in EIMS.

- (7) Enterprise Backend Attribute Exchange (BAE) Service. An enterprise BAE service must be established and maintained that:
- (a) Is compliant with the Federal guidance and specifications for BAE;
 - (b) Interfaces with other Federal Agency BAE service providers to share DOE identity information with other Federal Agencies; and
 - (c) Provides DOE Elements a singular authoritative source for identity information of other Federal Agencies to conduct DOE business.

c. Credentials.

- (1) HSPD-12 Credentials. HSPD-12 Credentials are the Federal identification credentials that are compliant with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated 8-2013, or its successor. [See DOE O 472.2A, Personnel Security, Appendix G for further information on Personal Identity Verification (PIV).] The terms “HSPD-12 credentials” and “PIV cards” are used interchangeably within this Order.
- (a) DOE HSPD-12 credentials (PIV card) are the property of the U.S. Government and must be recovered whenever an individual has terminated employment or their security clearance status changes or otherwise no longer requires a badge.
 - 1 HSPD-12 Credentials must be issued to all Federal employees and contractor employees who require long term (greater than six months) physical access to DOE facilities or information systems.
 - 2 Issuance of HSPD-12 Credentials to DOE employees or contractor employees who are employed or providing services for less than 6 months must be based on a risk analysis.
 - (b) Processes and procedures for the issuance of DOE HSPD-12 Credentials must be specified in the DOE PIV Card Issuer (PCI) Operations Plan per NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs)*, dated 6-2008, or its successor. HSPD-12 Credential role holders facilitate credential issuance, maintenance, and lifecycle management.
 - 1 FIPS 201-2 specifies required separation of duties relative to the HSPD-12 Credential issuance process.

2 DOE Implementation of HSPD-12 credential-related tasks and assignment of roles will be defined in the PCI Operations Plan.

3 Authorizing the issuance of HSPD-12 Credentials is a Federal function.

(2) DOE Security Badges. The HSPD-12 Credential is the DOE security badge. DOE O 473.1, *Physical Protection Program*, current version, establishes requirements for usage of the DOE security badge.

(3) Other Government Agencies (OGA). HSPD-12 Credentials issued by OGAs must be accepted for identification of individuals as though it was issued by DOE. DOE shall not issue HSPD-12 Credentials to Federal employees from OGAs that issue HSPD-12 Credentials, including the Department of Defense (DoD), without approval from the Office of Environment, Health, Safety and Security (EHSS).

(4) Other Badges. The issuance of other badges to include LSSO badges, is specified in DOE O 473.1, current version.

d. Authentication and Authorization.

(1) Enterprise Access Management Service (EAMS). An enterprise access management service must be developed and offered as a Department-wide service that:

(a) Centralizes the authentication of individuals requiring access to DOE information systems.

(b) Supports authentication credentials approved by the DOE Office of the Chief Information Officer (OCIO), which includes, at a minimum:

1 The DOE HSPD-12 Credential;

2 HSPD-12 Credentials from OGAs;

3 Personal Identity Verification Interoperability (PIV-I) credentials; and

4 Federated identity credentials from identity providers certified under the Trust Framework Provider Adoption Process (TFPAP).

(2) DOE Information Systems. DOE information systems must ensure that the credential used for authentication meets the minimum level of assurance (LOA) requirements, which are determined by conducting an electronic

authentication risk assessment per OMB M-04-04 in conjunction with a FIPS-199 assessment.

- (a) New DOE Information Systems. New DOE information systems must accept the following credentials if presented by the user and the credential meets or exceeds the LOA of the system:
 - 1 An HSPD-12 Credential for DOE employees and contractor employees who possess an HSPD-12 Credential as required by this Order;
 - 2 An HSPD-12 Credential for Federal employees and contractor employees from other government agencies;
 - 3 A PIV-I credential; and
 - 4 A federated identity credential from an identity provider certified under the TFPAP.
- (b) Existing DOE Information Systems. Existing DOE information systems must be upgraded to accept the credentials in 4d(2)(a), as appropriate, using the Risk Management Approach per DOE O 205.1, *Department of Energy Cyber Security Program*, current version.
- (c) System Specific Credentials. DOE information system owners may issue and manage credentials for authentication ONLY when:
 - 1 The individual does not possess or have access to one of the credentials in 4d(2)(a); or
 - 2 The DOE information system requires individuals to authenticate with a credential in addition to the credentials in 4d(2)(a).
- (d) DOE Headquarters Information Systems. DOE Headquarters information systems owned and operated by DOE Headquarters Staff Offices or by contractors on behalf of DOE Headquarters Staff Offices must use the EAMS for authentication.

(3) DOE Facilities.

- (a) Access control decisions are based on risk management principles as required by the current versions of DOE O 473.1 and DOE O 470.4, *Safeguards and Security Program*.
- (b) Access control processes must accept for authentication the following credentials:
 - 1 An HSPD-12 Credential for DOE employees and contractor employees;
 - 2 An HSPD-12 Credential for Federal employees and contractor employees from other government agencies;
 - 3 A PIV-I credential; and
 - 4 Other badges to include LSSO badges, as specified in DOE O 473.1, current version.
- (c) Automated access control systems should obtain authoritative data from the EIMS.
- (d) DOE O 473.1, current version, contains the requirements for access control systems.
- (4) Background Investigations. This Order does not impose background investigation requirements for authentication and authorization to DOE facilities or DOE information systems.
- (5) Authorization. Authorization to access a DOE facility or a DOE information system is inherently a risk-based decision.

e. Privilege Management.

- (1) DOE employees and contractor employees must have access to a DOE information system and/or DOE facility:
 - (a) To which they are entitled for the performance of official duties; and
 - (b) Only for the time period or duration in which they require it.
- (2) Enterprise Privilege Management Service. An enterprise access privilege service must be developed and offered as a Department-wide service that:
 - (a) Streamlines and automates the tasks associated with provisioning, updating, and deprovisioning access to DOE facilities and information systems that integrate with it; and

- (b) Streamlines and automates the issuance and maintenance of HSPD-12 Credentials and other credentials covered in this Order.

f. Public Key Infrastructure (PKI).

- (1) Public Key Infrastructure (PKI) certificates for authentication, encryption, and signing operations must be issued by a PKI that operates in compliance with the current X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework where intra- and inter-agency interoperability and trust is required.
- (2) A DOE PKI must be implemented as an enterprise service that:
 - (a) Is cross-certified or chained through an approved Shared Service Provider (SSP) with the U.S. Federal PKI Common Policy Framework;
 - (b) Issues PKI certificates to DOE employees and contractor employees where intra- and inter-agency interoperability and trust is required; and
 - (c) Operates under the direction of the DOE PKI Policy Management Authority (PMA).
- (3) DOE Elements may implement internal (or local), site-specific PKIs to satisfy local PKI requirements that do not require trust and interoperability outside of site-specific locations. These local PKIs are not subject to the direction of the DOE PKI PMA; however, local PKIs must adhere to the Risk Management Approach per DOE O 205.1, current version, especially with respect to non-repudiation.

g. Digital Signatures and Encryption.

- (1) DOE Elements must enable use of the PKI certificates to digitally sign and encrypt emails, business transactions, and relevant business documents in those cases where digital signatures and/or encryption are required.
- (2) Digital signatures should be created with HSPD-12 Credentials, when practical.

h. PIV FILES. All documentation created in the PIV process will be retained in files with unique file identification. PIV case files must be distinct from personnel security (access authorization) files. When a PIV decision is linked to a personnel security determination, the personnel security file (PSF) is only used for documentation of the personnel security process, not the identity-proofing process. The System of Record numbers for PIV files are DOE-63, Personal Identity Verification files and GSA/GOVT-7 HSPD 12 USAccess.

10-28-2024

5. RESPONSIBILITIES.

- a. Lead Program Secretarial Officers (LPSOs). Lead Program Secretarial Officers (LPSOs) shall perform risk analysis per paragraph 4.c.(1)(b) to authorize the issuance of HSPD-12 Credentials to Federal employees and contractor employees at their sites whose term of service is less than 6 months.
- b. Heads of Departmental Elements. Heads of Departmental Elements shall:
 - (1) Have overall responsibility for the implementation of DOE's identity, credential, and access management program for their respective elements.
 - (2) Establish written procedures within their organizations with clear lines of responsibility for implementing the requirements of this order, including but not limited to:
 - (a) The issuance, use, suspension, recovery, and destruction of the DOE HSPD-12 credential.
 - (b) Maintaining current and accurate employee information in PIV databases.
 - (c) Frequent verification that access to logical systems and physical facilities has been removed for individuals who no longer have an official relationship with the Department.
 - (3) Approve the issuance of Local Site-Specific Only (LSSO) badges to non-U.S. nationals who have resided in the U.S. for less than three years, based on a risk determination, and after the completion of the required background checks.
 - (4) Designate responsible individuals to work with the DOE Office of Management, Office of Acquisition and Project Management (OAPM) and the NNSA Office of Acquisitions and Supply Management (OASM) in providing procurement policy and guidance to contracting officers as follows:
 - (a) Identify and add the CRD of this Order to applicable existing and new contracts; and
 - (b) Ensure coordination with the applicable ICAM professionals to monitor and ensure contractor compliance with the CRD requirement during performance.
 - (5) Ensure that personal information collected for employee and contractor identification is handled in accordance with the Privacy Act of 1974, DOE O 206.1, *Department of Energy Privacy Program*, current version, and DOE O 471.7, *Controlled Unclassified Information*, current version.

- c. DOE Office of the Chief Information Officer (OCIO). The OCIO shall:
 - (1) Serve as the Agency Lead for ICAM and is responsible for managing and tracking the execution of the DOE ICAM program.
 - (2) Establish an Integrated Project Team (IPT) with representatives from the DOE Elements to ensure that the execution of the ICAM initiative is a coordinated and collaborative approach.
 - (3) Ensure that Enterprise ICAM Services are developed and provided.
 - (4) Appoint the DOE PKI PMA.
 - (5) Approve credentials that the EAMS will support.
- d. Office of Environment, Health, Safety, and Security (EHSS). EHSS shall:
 - (1) Oversee issuance and maintenance of the HSPD-12 Credentials for DOE Headquarters.
 - (2) Publish and maintain the DOE PCI Operations Plan.
 - (3) Maintain DOE access control and physical security policies.
 - (4) Determine the issuance of HSPD-12 Credentials to Federal employees and contractor employees at DOE Headquarters whose term of service is less than 6 months.
- e. DOE ICAM Integrated Project Team (IPT). The IPT shall:
 - (1) Work with the OCIO to ensure that program-level decisions are based on coordinated input from all the stakeholders.
 - (2) Publish and maintain a DOE Federated ICAM Framework in order to define the goals and objectives for achieving a DOE ICAM target state that is consistent with this policy, national policy and Federal ICAM guidance, and in a manner that improves, rather than impedes, the fulfillment of the Department's statutory missions.
 - (3) Ensure that the enterprise requirements specified in paragraph 4 Requirements, (above) are fulfilled to satisfy DOE cross enterprise needs.
- f. DOE Contracting Officials. DOE Contracting Officials shall:
 - (1) Incorporate the CRD into affected contracts unless other policy directions are provided by OAPM or OASM under paragraph 5.b.(1) of this Order.
 - (2) Work in partnership with ICAM professionals or the Contracting Officer Representative, as appropriate, to ensure that applicable ICAM scope,

clauses, and the CRD are incorporated into contracts; and to ensure contractor compliance with the ICAM requirements during performance.

6. REFERENCES.

- a. Executive Office of the President, Homeland Security Presidential Directive 12, August 27, 2004, <https://www.opm.gov/news/reports-publications/management-budget-reports/homeland-security-presidential-directive-hspd-12.pdf>
- b. Executive Office of the President, National Strategy for Trusted Identities in Cyberspace (NSTIC), April 2011.
https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- c. Executive Office of the President, White House Cyberspace Policy Review, May 2009,
https://www.energy.gov/sites/default/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf
- d. Federal Acquisition Regulation 52.204-9, Personal Identity Verification of Contractor Personnel <https://www.acquisition.gov/far/52.204-9>
- e. OMB Memorandum 04-04, E-Authentication Guidance for Agencies, December 2003.
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf>
- f. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf>
- g. OMB Memorandum 11-11, Continued Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011.
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf>
- h. OMB Memorandum 19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019.
<https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>
- i. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006,
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-18.pdf>

- j. OMB Memorandum, Requirements for Accepting Externally-Issued Identity Credentials, October 6, 2011,
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/ombreqforacceptingexternally_issuedidcred10-6-2011.pdf
- k. FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013,
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>
- l. Office of Personnel Management (OPM) Memorandum, subject: Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008, (2008 Final Credentialing Standards)
<https://www.opm.gov/suitability/suitability-executive-agent/policy/final-credentialing-standards.pdf>
- m. OPM Memorandum, subject: Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials, December 15, 2020, (2020 Credentialing Standards Procedures)
<https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf> DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, current version
- n. Performance Accountability Council (PAC) Memorandum, subject: Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism, March 02, 2016, (2016 PAC Memorandum) <https://www.opm.gov/suitability/suitability-executive-agent/policy/memo-issuing-piv-credentials-and-suspension-criteria.pdf>
- o. Joint Federal Investigations Notice and Suitability and Credentialing Executive Agent Notice/NBIB Notice No.18-02 Suit/Cred EA Notice No.18-01 dated April 05, 2018,
<https://www.dcsa.mil/Portals/91/Documents/pv/GovHRSec/FINs/FY18/fin-18-02.pdf>
- p. DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, current version
- q. DOE O 470.4, *Safeguards and Security Program*, current version
- r. DOE O 471.7, *Controlled Unclassified Information*, current version
- s. DOE O 473.1, *Physical Protection Program*, current version
- t. DOE Federated ICAM Framework, June 30, 2011,
https://powerpedia.energy.gov/wiki/Doe_federated_icam_framework

- u. X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, <https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf>

7. DEFINITIONS.

- a. **Adjudicator:** The Adjudicator is a federal employee delegated the duty to review and adjudicate all federal employee and contractor background investigations. The Adjudicator enters or updates the adjudication results for applicants in the credential issuance system.
- b. **Applicant:** An individual applying for an HSPD-12 Credential. The applicant may be a current or prospective Federal hire or a Federal employee or an applicant for employment with a DOE contractor or a current DOE contractor employee.
- c. **Authentication:** The process of verifying a person's identity using a credential (password, PIN, smartcard, badge, etc). The Physical Access community may use the term "validate & verify" a credential, which is an equivalent operation.
- d. **Authoritative Data Source:** A repository or system that contains identity information about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or conflicting data, the identity information within the authoritative data source is considered to be the most accurate.
- e. **Authorization:** The processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities. Once a person is authenticated, the system determines the appropriate set of privileges (or access) for that individual.
- f. **DOE facility:** A facility, which is owned (or leased) and operated by DOE or by contractors on behalf of DOE, that is required by DOE O 473.1, current version, to have access control.
- g. **DOE information system:** An information system that is owned and operated by DOE or by contractors on behalf of DOE to accomplish a Federal function. Regardless of whether DOE Federal employees have access, this does not include information systems operated by M&O contractors unless such systems' primary purpose is to accomplish a Federal function.
- h. **HSPD-12 Credential:** The HSPD-12 Credential is the Personal Identity Verification Card (or PIV Card) as mandated by Homeland Security Presidential Directive 12 (HSPD-12).
- i. **Issuer:** The organization that is issuing the HSPD-12 Credential to an applicant.
- j. **Level of Assurance:** As described in OMB M-04-04, level of assurance (or LOA) is the degree of certainty that a credential used for authentication actually refers to the identity of the person who is using the credential.

- k. **Personal Identity Verification Interoperability (PIV-I):** PIV-I is a credential that is issued to non-Federal entities per *Personal Identity Verification Interoperability for Non-Federal Issuers* dated July 2010, to facilitate interactions with Federal Government facilities and information systems.
 - l. **Sponsor:** The individual who substantiates the current, active DOE employment status of the individual and the need for an HSPD-12 Credential to be issued to an applicant, enters the applicant's required biographical and sponsorship data elements into the credential issuance system, and remains aware of the applicant's status and continuing need for holding an HSPD-12 Credential.
8. CONTACT. Office of the Chief Information Officer, 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:



DAVID M. TURK
Deputy Secretary

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 206.2, *IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

1. GENERAL.

- a. DOE facilities and DOE information systems must meet the requirements of Office of Management and Budget (OMB)M-19-17, which requires that agency implementations align with the Federal Chief Information Officers Council's *Federal Identity Credential Access Management (FICAM) Roadmap and Implementation Guidance* and the FICAM Architecture and Continuous Diagnostics and Mitigation (CDM).

PIV credentials (where applicable in accordance with OPM requirements) are DOE's primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors.

- b. HSPD-12 Credentials. HSPD-12 Credentials are the Federal identification credentials that are compliant with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated 8-2013, or its successor. Contractor employees requiring an HSPD-12 Credential are subject to Personal Identity Verification (PIV) by DOE.

- (1) This Order establishes the requirement for issuance of PIV to federal employees and contractors.
 - (a) Local implementation of the requirements under the DOE authorization to issue PIV credentials using the DOE provider, USAccess, may be performed by an M&O contractor.
 - (b) An M&O contractor may serve as the sponsor for M&O staff and subcontractors for a PIV credential.
- (2) HSPD-12 Credentials must be issued to all Federal employees and contractor employees who require long term (greater than six months) physical access to DOE facilities or information systems.
- (3) Issuance of HSPD-12 Credentials to DOE employees or contractor employees who are employed or providing services for less than 6 months is at the discretion of the Lead Program Secretarial Officer (LPSO) and based on a risk analysis.

- c. Identity. Contractors may participate in the enterprise identity management service (EIMS) and should determine participation based on business value and risks. If participating, contractors must:
 - (1) Identify their authoritative data sources to the DOE registry of authoritative data sources; and
 - (2) Make available identity information from authoritative data sources to the EIMS.
 - d. Electronic Transactions with DOE. When DOE requires digital signatures or encryption, contractors must enable the use of Public Key Infrastructure (PKI) certificates.
 - (1) The PKI must comply with the current X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
 - (2) Contractors should use the PKI certificates that are on the HSPD-12 Credential, when practical.
2. DOE INFORMATION SYSTEMS. When operating a DOE information system as defined in this Order, the contractor must meet the following requirements.
- a. General. DOE information systems must meet the requirements of Office of Management and Budget (OMB) M-19-17, which requires that agency implementations align with the Federal Chief Information Officers Council's *Federal Identity Credential Access Management (FICAM) Roadmap and Implementation Guidance*, and the FICAM Architecture and Continuous Diagnostics and Mitigation (CDM).
 - b. Authentication and Authorization.
 - (1) DOE information systems must ensure that the credential used for authentication meets the minimum level of assurance (LOA) requirements, which are determined by conducting an electronic authentication risk assessment per OMB M-04-04 in conjunction with a FIPS 199 assessment.
 - (a) New systems must accept the following credentials if presented by the user and the credential meets or exceeds the LOA of the system:
 - 1 An HSPD-12 Credential for DOE employees and contractor employees who possess an HSPD-12 Credential as required by this Order;
 - 2 An HSPD-12 Credential for Federal employees and contractor employees from other government agencies;

3 A Personal Identity Verification Interoperability (PIV-I) credential; and

4 A federated identity credential from an identity provider certified under the Trust Framework Provider Adoption Process (TFPAP).

(b) Existing DOE information systems must be upgraded to accept the credentials in 2b(1)(a), as appropriate, using the Risk Management Approach per DOE O 205.1, *Department of Energy Cyber Security Program*, current version.

(2) DOE information system owners may issue and manage credentials for authentication ONLY when:

(a) The individual does not possess or have access to one of the credentials in 2b(1)(a); or

(b) The DOE information system requires individuals to authenticate with a credential in addition to the credentials in 2b(1)(a).

3. DOE FACILITIES.

a. Access control decisions are based on risk management principles as required by the current versions of DOE O 473.1, *Physical Protection Program*, and DOE O 470.4, *Safeguards and Security Program*.

b. Contractors must recognize the following credentials as an acceptable credential for verifying a person's identity as part of the site's physical access procedure:

(1) An HSPD-12 Credential for DOE employees and contractor employees;

(2) An HSPD-12 Credential for Federal employees and contractor employees from other government agencies; and

(3) A PIV-I credential.

c. Automated access control systems should obtain authoritative data for DOE employees and contractor employees external to the site from the EIMS offered by DOE.

d. DOE O 473.1, current version, contains the requirements for access control systems.