SUPPLEMENTAL DIRECTIVE

NNSA SD 206.2

Approved: 4-14-18
Certification Due: 4-14-21

IMPLEMENTATION OF PERSONAL IDENTITY VERIFICATION FOR UNCLEARED CONTRACTORS

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
https://www.energy.gov/nnsa/nnsa-policies-and-directives

OFFICE OF PRIMARY INTEREST (OPI):
Office of Defense Nuclear Security

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

IMPLEMENTATION OF PERSONAL IDENTITY VERIFICATION FOR UNCLEARED CONTRACTORS

1. PURPOSE. To establish supplemental requirements and responsibilities for the National Nuclear Security Administration's (NNSA) implementation for Personal Identity Verification (PIV) under Department of Energy (DOE) Order (O) 206.2, *Identity, Credential, and Access Management (ICAM)* that:

   (1) Identify NNSA contractors subject to PIV processing;

   (2) Identify the standards applied to PIV determinations;

   (3) Establish responsibilities for PIV processes; and

   (4) Provide a process for reconsideration (appeal).

2. CANCELLATION. None.

3. APPLICABILITY.

   a. Federal. This Supplemental Directive (SD) applies to all NNSA organizations serviced by the Office of Personnel and Facility Clearances and Classification (OPFCC). This directive does not apply to federal employees requiring PIV processing.

   b. Contractors. The Contractor Requirements Document (CRD), provided as Attachments 1-3, sets forth requirements of this directive that apply to all NNSA contractors. The CRD must be included in contracts when:

      (1) Contractor employees require physical access to NNSA sites; or

      (2) Contractor employees require logical access, including remote access, to NNSA information technology (IT) systems.

   c. Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 United States Code (U.S.C.) sections 2406 and 2511, and to ensure consistency throughout 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.

4. SUMMARY OF CHANGES. Not applicable.

5. BACKGROUND. This directive implements the requirements contained in National and Departmental policy for PIV processing. The directive supplements existing requirements contained in DOE O 206.2 Appendix A, specifically, the PIV appeal processes and processing times.

   a. Homeland Security Presidential Directive (HSPD)-12 mandates the development and implementation of a Government-wide standard for secure and reliable forms of identification to be issued to federal employees and contractors. Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, defines a reliable, Government-wide PIV system. It also includes an identity proofing process based on a background investigation and issuance of a common identification badge.

   b. Office of Management and Budget (OMB) Implementation Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, provides guidance for implementing the requirements in FIPS 201-2 and HSPD-12. The memorandum clarifies who is subject to PIV processing and establishes the basis for reciprocal acceptance of PIV decisions made by other agencies.

   c. Joint Memorandum from the OMB, the Office of Personnel Management (OPM), and the Office of the Director of National Intelligence, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, dated 3-2-16, reaffirmed OPM's guidance issued in the 2008 memo, *Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12*.

6. REQUIREMENTS.

   a. Contractors who require physical access to NNSA sites greater than 179 days must be processed for PIV. Contractors who require logical access, which includes remote access, to NNSA IT systems greater than 179 days must be processed for PIV. This includes any physical and logical access combination greater than 179 days.

   b. This SD does not preclude requesting a PIV for an individual when access is less than 179 days.

   c. The Office of Personnel and Facility Clearances and Classification (OPFCC) must apply the credentialing standards set forth in Attachment 2.

   d. OPFCC must issue a written decision to the individuals and notify the applicable federal office, which will immediately notify the contractor.

   e. NNSA may accept a favorably adjudicated Tier 1 or equivalent background investigation from any government entity.

f. At a minimum, a Tier 1 background investigation must be performed for all uncleared contractors to whom this directive applies. As outlined in Attachment 1, site contractors should begin the PIV process as soon as a person accepts an offer of employment. Individuals must complete the appropriate standard form (SF) -85 investigation forms on-line through OPM's Electronic Questionnaire for Investigations Processing (e-QIP) application site.

g. Foreign Nationals.

(1) Foreign Nationals (FN) must not undergo the PIV process. They must be reviewed according to DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*, or successor directive.

(2) NNSA must not reciprocally accept PIV determinations on FNs due to existing laws and Departmental requirements.

h. OPFCC must implement an appeal process for individuals who have been denied a PIV.

i. If derogatory information arises, the Officially Designated Federal Security Authority (ODFSA) must act according to local procedures. Derogatory information does not affect the initial favorable adjudication for a PIV.

j. Within 2 working days the OPFCC must provide the individual reasonable notice of the denial determination. The notice must also include the reason(s) for the denial determination. The notice must state:

(1) The specific reason(s) for the determination.

(2) The individual’s right to appeal in writing.

(3) The information the individual is required to address.

(4) The time limit (i.e., 15 calendar days) in which the individual has to respond/appeal.

(5) The address to which the response/appeal must be sent.

k. Contractors may be issued an HSPD-12 PIV credential only when the required Tier 1 or equivalent background investigation has been favorably adjudicated.

l. Annual/periodic assessments of the ODFSA must analyze the implementation of this SD for adherence to all requirements.

m. Requirements that cannot be implemented within 6 months of the effective date of this NNSA policy, or with existing resources, must be documented by the ODFSA and provided to the Chief, Defense Nuclear Security. The documentation must include timelines and resources needed to fully implement this NNSA policy.

The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.

7. RESPONSIBILITIES.

a. Chief, Defense Nuclear Security (CDNS) (NA-70).

(1) Serves as the DOE cognizant security officer responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA.

(2) Approves or disapproves equivalencies to this SD requested by the ODFSA.

b. NNSA Chief Information Officer (NA-IM).

(1) Serves as the DOE cognizant security officer responsible for the development and implementation of cybersecurity program and IT operations under the purview of NNSA.

(2) Approves or disapproves equivalencies to this SD requested by NNSA field offices involving logical access.

c. Director, Office of Personnel and Facility Clearances and Classification (OPFCC) (NA-74).

(1) Implements the PIV determination process.

(2) Implements an appeal process for individuals who have been denied a PIV determination.

d. Officially Designated Federal Security Authority (ODFSA).

Monitors contractor implementation of this Supplemental Directive.

e. Contracting Officers.

Incorporates Attachment 1, the Contractor Requirements Document in contracts.

8. REFERENCES. See Attachment 3.

9. CONTACT. Office of Defense Nuclear Security (NA-70), 202-586-8900.

BY ORDER OF THE ADMINISTRATOR:

Lisa E. Gordon-Hagerty
Administrator

Appendix 1. Definitions

Attachments:
1. Contractor Requirements Document
2. PIV Credentialing Standards
3. References

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 1: DEFINITIONS

Note: These terms are defined in relation to this Supplemental Directive.

a. Access control: The process of determining the permissible activities of users and authorizing or prohibiting activities by each user. Controlling a user's access to facilities and computer systems includes setting rights and permissions that grant access only to authorized users. There are two types of access control—physical access and logical access:

- Physical access control focuses on restricting the entry or exit of users from a physical area, such as a building or a room in a building.
- Logical access control is used to determine what electronic information and systems users and other systems may access and what may be done to the information that is accessed.

b. Adjudicate: The act of making a judgment regarding a person or about a situation based on an established, formal process.

c. Adjudication: An evaluation of pertinent data contained in a background investigation, as well as any other relevant information made available, to determine whether an individual is eligible for access to National Nuclear Security Administration (NNSA) information technology (IT) systems or facilities.

d. Enrollment station: Equipment used to capture the Personal Identity Verification (PIV) applicant's required information, including biographical data, identity documents, photograph, fingerprints, and biometric fingerprint image. This equipment typically consists of a computer monitor/keyboard, personal identification number (PIN) pad, document scanner, camera, network connection, back-end database, and software.

Homeland Security Presidential Directive (HSPD)-12 Credential enrollment stations are located in Department of Energy (DOE) Badge offices. A fixed enrollment station is a permanent location with a General Services Administration-provided computer, equipment, and operator who handles enrollment and activation of DOE HSPD-12 credentials (also handles PIN resets).

e. Officially Designated Federal Security Authority (ODFSA): Federal employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation.

Delegation authority for these positions is originated according to direction from the accountable Program Secretarial Officer (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Office), who also provides direction for which of the ODFSA positions may be further delegated. Each delegation must be documented in writing. The delegation may be included in other security plans or documentation approved by or according to direction from the

accountable principal. Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation.

f. NNSA Information Technology (IT) System: An information system that is owned or operated by NNSA or by contractors on behalf of NNSA to accomplish a federal function. Regardless of whether NNSA federal employees have access, this does not include information systems operated by Management and Operating (M&O) contractors unless such systems' primary purpose is to accomplish a federal function.

g. PIV Determination (suitability): A decision by NNSA that a person is suitable or not suitable to possess a PIV.

h. Reciprocity: Mutual exchange and acceptance of a PIV determination made by another entity.

i. Tier 1 Background Investigation: Investigations designated for low risk, non-sensitive positions, including HSPD-12 credentialing. These investigations require the use of the Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions or use of appropriate e-QIP version. Tier 1 investigations should not be confused with Tier 3 or 5 investigations required for access to classified matter of nuclear material which have significantly longer processing times.

j. Uncleared Contractor: A contract employee not requiring access to classified matter of nuclear material.

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT
SD-206.2, *IMPLEMENTATION OF PERSONAL IDENTITY VERIFICATION FOR UNCLEARED CONTRACTORS*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary for compliance with the requirements.

1. REQUIREMENTS.

   a. Contractors who require physical access to National Nuclear Security Administration (NNSA) sites greater than 179 days must be processed for Personal Identity Verification (PIV). Contractors who require logical access, which includes remote access, to NNSA information technology (IT) systems greater than 179 days must be processed for PIV. This includes any physical and logical access combination greater than 179 days.

   b. This Supplemental Directive does not preclude individuals from undergoing a PIV when access is less than 179 days.

   c. Contractors may be issued a Homeland Security Presidential Directive (HSPD)-12 PIV credential only when the required Tier 1 or equivalent background investigation has been favorably adjudicated.

   d. Uncleared contractors must be subject to the minimum and the supplemental PIV credentialing standards set forth in Attachment 2.

   e. Investigation Requirements.

      (1) A Tier 1 investigation or equivalent is the minimum requirement.

      Note: Reinvestigations for PIV determinations are not required.

      (2) NNSA contractors must designate the proper position sensitivity using the Office of Personnel Management (OPM) Position Designation Tool.

      (3) NNSA contractors must provide the standard form (SF)-85, *Questionnaire for Non-Sensitive Positions*, and related documents needed to conduct a Tier 1 investigation to the Office of Personnel and Facility Clearances and Classification (OPFCC) via OPM's Electronic Questionnaire for Investigations Processing (e-QIP).

      (4) The individual must be sponsored in the US Access system prior to using the enrollment station for the fingerprint check. NNSA contractors must use the enrollment station to capture fingerprints to be sent to OPM. OPFCC will provide fingerprints for processing.

f. Approvals of PIV determinations are final and are not subject to further investigation.

g. Denial of PIV determination for uncleared contractors.

(1) OPFCC Notification. When the Adjudicator determines that an individual has not provided his or her verifiable identity, or is found unsuitable, OPFCC must provide the individual reasonable notice of the determination including the reason(s) within 2 working days. The notice must state:

(a) The specific reason(s) for the determination.

(b) The individual's right to appeal in writing.

(c) The information the individual is required to address.

(d) The time limit (i.e., 15 calendar days) in which the individual has to respond/appeal.

(e) The address to which the response/appeal must be sent.

(2) Response. The individual has 15 calendar days from receipt of the OPFCC notification to respond/appeal. The individual must respond/appeal in accordance with the OPFCC notification.

h. Final Decision.

(1) If the individual fails to respond within 15 calendar days, OPFCC will issue a formal decision of denial to the individual. The Officially Designated Federal Security Authority (ODFSA) will also be notified of the decision and will immediately notify the contractor. The individual must be denied physical access to NNSA sites and logical access to NNSA IT systems.

(2) If the individual provides a written response for the appeal process, OPFCC must consider the information prior to rendering a final determination. OPFCC will issue a written decision to the individual and notify the applicable federal office, which will immediately notify the contractor.

(a) If the individual receives a favorable determination, a PIV credential may be issued.

(b) If the individual receives an unfavorable determination, a PIV credential must not be issued and the individual must be denied physical access to NNSA sites and logical access to NNSA IT systems.

1 The contractor is responsible for immediately removing the individual from the worksite and ensuring the immediate disabling of the individual's access to all NNSA IT systems, including remote access.

2 Specific details regarding the suitability issues will not be provided to the contractor. The PIV credentialing standards (Attachment 2) applied to the individual's denial may be provided to the ODFSA upon request.

(3) Contractors cannot request a subsequent PIV for an individual until 1 year after the decision date. The reconsideration decision is not subject to further appeal.

i. Foreign Nationals.

(1) Foreign Nationals (FN) must not undergo the PIV process. They must be reviewed according to DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*, or successor directive.

(2) OPFCC must not reciprocally accept PIV determinations on FNs due to existing laws and Departmental requirements.

j. Subsequent information and reportable items must not be reported to OPFCC because the PIV program does not include a requirement for continuous evaluation.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2: PERSONAL IDENTITY VERIFICATION CREDENTIALING STANDARDS

Note: This attachment applies to NNSA federal and contractor organizations.

1. Minimum Homeland Security Presidential Directive (HSPD)-12 Personnel Identity Verification (PIV) credentialing standards. In accordance with Office of Personnel Management (OPM) guidelines, a PIV card will not be issued to a contractor if any of the following applies:

    a. The individual is known to be, or reasonably suspected of being, a terrorist;

    b. The employer is unable to verify the individual's claimed identity;

    c. There is a reasonable basis[1] to believe that the individual has provided fraudulent information concerning his or her identity;

    d. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the *Privacy Act*, information that is proprietary in nature, or other sensitive or protected information;

    e. There is a reasonable basis to believe the individual will use an identity credential outside the workplace or inappropriately;

    f. There is a reasonable basis to believe the individual will use federally controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

2. Supplemental HSPD-12 PIV Card Credentialing Standards.

    a. Supplemental standards are intended to make certain that the issuance of a PIV credential to an individual does not create an unacceptable risk, when the individual is not subject to an adjudication of suitability for employment in the competitive service under 5 CFR part 731, of qualification for employment in the excepted service under 5 CFR part 301 or under a similar authority, or of eligibility for access to classified information under Executive Order 12968.

    b. A PIV credential may be denied or revoked based on one of the supplemental credentialing standards listed under this paragraph. In the following standards, an *unacceptable risk* refers to a risk to life, safety, or health of employees,

[1] A reasonable basis to believe occurs when a disinterested observer, with knowledge of the same facts and circumstances, would reasonably reach the same conclusion.

contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical; or to the privacy of data subjects.

c. The following standards must be applied to contractors not subject to federal suitability or security clearance adjudication.

(1) There is a reasonable basis to believe:

(a) based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;

(b) based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

(c) based on the individual's material, intentional false statement, deception, or fraud in connection with contract employment, that issuance of a PIV card poses an unacceptable risk;

(d) based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk; and

(e) based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(2) A statutory or regulatory bar prevents the individual's contract employment; or would prevent federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or

(3) The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

ATTACHMENT 3: REFERENCES

Note: This attachment applies to NNSA federal and contractor organizations.

a. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated 8-27-04

b. U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB 201-2), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated August 2013

c. Office of Management and Budget (OMB) Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated 8-5-05

d. Office of Personnel Management (OPM) Memorandum, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*, dated 7-31-08

e. Joint Memorandum from the Office of Management and Budget, the Office of Personnel Management, and the Office of the Director of National Intelligence, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, dated 3-2-16

f. DOE O 142.3A Chg. 1, *Unclassified Foreign Visits and Assignments Program*, dated 1-18-17

g. DOE O 206.2, *Identity, Credential, and Access Management (ICAM)*, dated 2-19-13

h. DOE O 470.4B Chg. 2, *Safeguards and Security Program*, dated 1-17-17