**ORDER**

**SPRPMO O 206.2**

**Approved: 6/02/16**

# MULTIFACTOR AUTHENTICATION

**U.S. DEPARTMENT OF ENERGY**
**Strategic Petroleum Reserve**
**Project Management Office**

**DISTRIBUTION**: All SPRPMO Employees, M&O, A-E, and Support Services Contractors

**INITIATED BY**: APM, Systems and Projects, Information Systems and Technical Services

**RESERVED**

# MULTIFACTOR AUTHENTICATION

1. PURPOSE. In accordance with Department of Energy (DOE) O 206.2, *Identity, Credential, and Access Management*, DOE Information Systems must ensure that the credential used for authentication meets minimum level of assurance (LOA) requirements. This Order establishes requirements for use of Personal Identity Verification (PIV) smart cards as the authentication mechanism to access Strategic Petroleum Reserve Project Management Office (SPRPMO) Information Systems.

   Homeland Security Presidential Directive 12 (HSPD-12) requires that Federal Government agencies use "secure and reliable forms of identification" to verify the identities of federal employees and contractors. Subsequently, the Department of Commerce issued Federal Information Processing Standard (FIPS) 201 that provides implementation instructions and standards for the Directive.

   Current federal direction and DOE-specific guidance requires authentication to SPRPMO information systems using multiple factors of authentication in place of, or in addition to, the traditional username and password combination. A combination of federally-issued PIV smart card and Personal Identification Number (PIN) code has been identified as the required authentication methodology where feasible.

2. CANCELLATION. None.

3. APPLICABILITY. This Order applies to all SPRPMO organizational elements, personnel, contractors, and visitors that enter SPRPMO facilities or that have access to SPRPMO information.

   a. SPRPMO Elements: This Order applies to all DOE/SPRPMO employees.

   b. DOE Contractors. Except for the exclusions in Paragraph 3c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements to be applied to the Management and Operating (M&O) Contractor, Support Services Contractor, and other contractors authenticating to SPRPMO information systems.

   c. Exclusions: None.

4. REQUIREMENTS.

a. General Authentication Requirements. SPRPMO Federal employees and contractors with information system accounts are required to authenticate (logon) to SPRPMO information systems using a combination of their federally-issued badge (i.e., PIV card) and associated PIN code where the capability has been implemented. The requirement applies to individuals that are in possession of a PIV card, and are accessing SPRPMO information systems using government-furnished equipment (GFE) with PIV card capability installed (e.g., laptops with built-in card readers, desktops with external card readers, conference room/kiosk computers with card readers, etc.).

b. Exceptions. The following exceptions are allowed to facilitate authentication to SPRPMO information systems where PIV card usage is not feasible.

(1) Individuals not issued a PIV card. Individuals who have been authorized to access SPRPMO information systems but have not been issued a PIV card or SPRPMO-specific smart card/badge may use alternative authentication mechanisms in accordance with existing policies and procedures. Examples are new employees awaiting PIV card issuance and temporary personnel, typically working for less than 6 months, who are not, issued PIV cards.

(2) Individuals accessing SPRPMO information systems from personally-owned equipment. Individuals with non-privileged accounts ("S" or "T" accounts) who access SPRPMO information systems from personally-owned computing systems must use alternative two-factor authentication mechanisms (e.g., RSA SecurID tokens) in accordance with existing policies and procedures. PIV cards are not authorized for use on personally-owned equipment.

(3) Individuals accessing SPRPMO information systems from GFE that does not have PIV card capability. Individuals who authenticate to SPRPMO information systems for which no mechanism to facilitate PIV card authentication has been implemented may continue to use alternative authentication credentials in accordance with existing policies and procedures. Examples of these types of GFE are typically mobile devices such as phones and tablets.

(4) Individuals that temporarily do not have possession of a PIV card. Individuals who typically authenticate to SPRPMO information systems from GFE using their PIV card may temporarily use alternative authentication credentials when they are not in possession of a PIV card (e.g., forgotten or lost PIV card, non-working PIV card, etc.). Usage of alternative authentication credentials must be in accordance with existing policies and procedures

5. REFERENCES.

a. HSPD-12, Policy for a Common Identity Standard for Federal Employees and Contractors.

b. Office of Management and Budget (OMB) M-05-24, Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

c. FIPS 201-2, PIV of Federal Employees and Contractors.

d. DOE O 206.2, Identity, Credential, and Access Management.

6. DEFINITIONS.

a. Multifactor Authentication. The process of using two or more articles to verify the identity of an individual. For example, SPRPMO individuals may use both a PIV card and a PIN code to verify their identity in order to authenticate to SPRPMO information systems.

b. Personally-owned computing systems. Computing systems that may be used to access SPRPMO information systems that are not government-owned.

c. RSA SecurID Token. Hardware-based token that is issued to some SPRPMO employees to be used to authenticate to SPRPMO information systems.

d. PIN Code. A personal identification number code, usually 4 to 8 digits in length, is associated with a PIV card, and is used by individuals to authenticate to information systems.

e. PIV Card. The Personal Identity Verification Card as mandated by Homeland Security Presidential Directive 12 (HSPD-12), also referred to as a HSPD-12 Credential. PIV cards are sometimes referred to as smart cards.

f. 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.

7. CONTACT. The SPR Chief Information Officer (Director, Information Systems and Technical Services) is the point of contact regarding this Order.

Project Manager
Strategic Petroleum Reserve

Attachment:
Attachment 1 – Contractor Requirements Document

**CONTRACTOR REQUIREMENTS DOCUMENT**
**SPRPMO O 206.2, MULTIFACTOR AUTHENTICATION**
**Dated 6/02/16**

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 to ensure the contractor's compliance with the requirements.

The contractor will:

1. Authenticate (logon) to SPRPMO information systems using a combination of their federally-issued badge (i.e., PIV card) and associated PIN code where the capability has been implemented. The requirement applies to individuals that are in possession of a PIV card, and are accessing SPRPMO information systems using government-furnished equipment (GFE) with PIV card capability installed (e.g., laptops with built-in card readers, desktops with external card readers, conference room/kiosk computers with card readers, etc.).

2. Following exceptions as allowed to facilitate authentication to SPRPMO information systems where PIV card usage is not feasible. Exceptions are defined as:

    a. Individuals not issued a PIV card. Individuals who have been authorized to access SPRPMO information systems but have not been issued a PIV card or SPRPMO-specific smart card/badge may use alternative authentication mechanisms in accordance with existing policies and procedures. Examples are new employees awaiting PIV card issuance and temporary personnel, typically working for less than 6 months, who are not issued PIV cards.

    b. Individuals accessing SPRPMO information systems from personally-owned equipment. Individuals with non-privileged accounts ("S" or "T" accounts) who access SPRPMO information systems from personally-owned computing systems must use alternative two-factor authentication mechanisms (e.g., RSA SecurID tokens) in accordance with existing

policies and procedures. PIV cards are not authorized for use on personally-owned equipment.

c. Individuals accessing SPRPMO information systems from GFE that does not have PIV card capability. Individuals who authenticate to SPRPMO information systems for which no mechanism to facilitate PIV card authentication has been implemented may continue to use alternative authentication credentials in accordance with existing policies and procedures. Examples of these types of GFE are typically mobile devices such as phones and tablets.

d. Individuals that temporarily do not have possession of a PIV card**.** Individuals who typically authenticate to SPRPMO information systems from GFE using their PIV card may temporarily use alternative authentication credentials when they are not in possession of a PIV card (e.g., forgotten or lost PIV card, non-working PIV card, etc.). Usage of alternative authentication credentials must be in accordance with existing policies and procedures.