UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

December 15, 2020

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: MICHAEL J. RIGAS
ACTING DIRECTOR,
U.S. OFFICE OF PERSONNEL MANAGEMENT
CREDENTIALING EXECUTIVE AGENT

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

Introduction

1. Homeland Security Presidential Directive 12 (HSPD-12) states the "U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees.)" In my role as the Credentialing Executive Agent, I am issuing the following credentialing standards procedures to promote defined goals in agency eligibility determinations to issue HSPD-12 personal identity verification (PIV) credentials for access to federally controlled facilities and information systems: the protection of the life, safety, property, or health of employees, contractors, vendors or visitors to Federal facilities; the protection of the Government's physical assets, information systems, records, including privileged, proprietary, financial or medical records; and the privacy of the individuals whose data the Government holds in its systems. OPM intends to achieve these outcomes by guiding PIV eligibility determinations through the issuance of this document. This document provides government-wide credentialing standards procedures to be used by all Executive Branch Departments and Agencies (D/As) in issuing, suspending, or revoking eligibility for HSPD-12 PIV credentials to their employees and contractor personnel, including those who are non-United States citizens.

2. These procedures are to be used with the governmentwide credentialing standards, currently the *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12* issued by OPM in July 2008 *(2008 Final Credentialing Standards)* and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, of March 2, 2016, as clarified by this memorandum, and any future iterations of such standards. The authority is referenced in section 2.5(c) of Executive Order (EO) 13467, as amended.

Applicability

1. Executive Branch D/As will use these procedures in conjunction with the credentialing standards for making all decisions regarding the eligibility of individuals for a PIV credential for physical or logical access to Federally controlled facilities and/or information systems, including Federal employees and employees of government contractors who are performing work for or on behalf of a Federal department or agency, members of the armed forces, non-appropriated fund employees, as well as specific categories of individuals that are unique to a particular agency, such as guest researchers, volunteers, intermittent employees, seasonal employees, or employees on temporary appointments likely to continue for at least six months.

a. For the purpose of this guidance, short term employment is employment of less than six (6) continuous months.

b. Although not required, D/A's should consider the benefits of PIV eligibility determinations for intermittent or temporary employees whose affiliation is repeatedly terminated and reinstated, and for any employees who are expected to serve intermittently over multiple years.

c. Intermittent employees with affiliation that extends beyond six continuous months are not considered "short-term." Similarly, seasonal employees, i.e., employees on permanent appointments who work a seasonal schedule of six months or more on a recurring basis are not considered "short-term.[1]"

d. Agencies may have specific categories of personnel such as guest researchers or volunteers who are unique to the agency. These credentialing standards procedures generally apply to such personnel unless they are short-term (i.e. less than six continuous months) employees, in which case the agency has discretion to vet those personnel for PIV credential based on risk and other factors, or to issue an alternative identity credential with appropriate restrictions and alternative security protections.

e. An alternative identity credential (such as the Personal Identity Verification Interoperability or PIV-I) is an identity credential that *does not meet the standards outlined in these procedures* and is visually and electronically distinguishable from PIV credentials (that *do* meet these requirements). The employing agency assumes all risk in managing alternative credentials, and alternative identity credentials are not reciprocally acceptable.

2. In addition to the requirements in this memorandum for vetting covered employees

[1]Per 5 CFR 340.401(a), Seasonal Employment means annually recurring periods of work of less than 12 months each year. Seasonal employees are permanent employees who are placed in nonduty/nonpay status and recalled to duty in accordance with preestablished conditions of employment. Short term employees on temporary appointments of less than six months thus should not be included in the definition of "seasonal" (even if hired, for the summer, for example).

for PIV credential eligibility, the PIV credential (card) itself is subject to the requirements of HSPD-12 and standards and guidelines developed by the National Institute of Standards and Technology (NIST) and promulgated by the Office of Management and Budget (OMB).[2]

3. These credentialing standards procedures do not apply to identity credentials associated with national security systems defined by 44 U.S.C. 3552(b)(6).[3] Also, within Department of Defense (DoD) and Department of State (DoS), the procedures do not apply to family members and other eligible beneficiaries or occasional visitors to Federal facilities to whom DoD and DoS would issue temporary identification.

4. These credentialing standards procedures shall not be deemed to limit the responsibility and power of an agency head to deny or terminate access to the facilities and information systems under their control in the interests of national security.

Adjudicative Guidelines for PIV Credential Eligibility

1. D/As must apply the Adjudicative Guidelines provided in 2008 Final Credentialing Standards, or any successor document, and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, of March 2, 2016, in order to determine whether to find an individual eligible for a Federal PIV credential permitting physical and logical access to federally controlled facilities and federally controlled information systems. D/As will determine whether:

a. There is proof that the person is who s/he says s/he is;

b. Terrorism or information technology security concerns exist; and

c. There are any other issues that indicate issuance of a PIV credential to an individual will pose an unacceptable risk to any of the following:

    i. The life, safety, property or health of employees, contractors, vendors or visitors to a Federal facility;
    ii. The Government's physical assets or information systems;
    iii. Records, including privileged, proprietary, financial or medical records; or

---

[2] *See* 15 U.S.C. 278g-3(a); 40 U.S.C. 11331; *see also* 44 U.S.C. 3553. Section 2.5(c)(ix) of Executive Order 13467, as amended, requires OPM to "consult to the extent practicable" with the agencies that have statutory responsibilities under these and other provisions related to PIV credentials. OPM conducted this consultation before issuing these Credentialing Standards Procedures.

[3] PIV credentials are governed by FIPS 201-2; a "compulsory and binding" standard issued under 40 U.S.C. 11331 for the security of Federal information systems. However, these procedures do not apply to "national security systems" defined in 44 U.S.C. 3552(b)(6). Under 44 U.S.C. 3553(a)(4), however, the standards for national security systems must be complementary "to the maximum extent feasible." Agencies with such systems will follow the physical and logical access requirements established for such systems.

iv. The privacy of the individuals whose data the Government holds in its systems.

2. Agencies may not waive, modify[4] or replace these guidelines.

Inherently Governmental Determinations

1. PIV credential eligibility determinations are inherently governmental functions that must be rendered only by U.S. Government personnel or appropriate automated government procedures as approved by the Credentialing Executive Agent.

2. To the maximum extent practicable, D/As must align PIV eligibility determinations with other personnel vetting determinations made by trained federal adjudicators. Individuals making PIV eligibility determinations must be investigated and adjudicated at a level commensurate with the responsibilities of the position as determined through application of the Position Designation System.[5]

Credentialing Eligibility Process – Timing of PIV Adjudicative Decisions

D/As will make PIV eligibility determinations using one of the following options:

1. **Option 1:** Interim PIV eligibility determination - Followed by final PIV eligibility determination (**Two-Step Process**)

    a. **Step 1.** ***Interim PIV eligibility determination*****:** If a D/A wishes to bring a new appointee or contract employee on board pending completion of the required background investigation[6] the D/A must first make an interim PIV eligibility determination. The D/A must ensure all of the following is complete before making a favorable interim PIV eligibility determination[7]:

        i. Presentation by the appointee or employee of two identity source documents[8], at least one of which is a Federal or State government-issued picture identification,

[4] Modification includes changes to augment, enhance, or add guidelines.
[5] https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/
[6] Refers to the investigation required for making a PIV eligibility determination, or applicable suitability/fitness and/or national security eligibility decision under 5 CFR part 731 or equivalent standards, or SEAD 4 guidelines issued based on EOs 12968 and 13467, as amended.
[7] This requirement supersedes the guidance listed in the 2008 Credentialing Standards.
[8] *See* Federal Information Processing Standards Publication (FIPS) 201-2 of August 2013, or subsequent issuance for additional guidance regarding identity source documents. Also see the list of acceptable documents for new employment verification included in Form I-9, *Employment Eligibility Verification.*

ii. Favorable review[9] by the D/A of the intended PIV recipient's completed investigative questionnaire,[10]
iii. Initiation of the intended PIV recipient's required background investigation (Tier 1 or higher) request, meaning the D/A has submitted the request for investigation to the Federal background investigation service provider (ISP), and the ISP has scheduled the investigation; and
iv. Favorable review[11] by the D/A of the results of the intended PIV recipient's FBI National Criminal History Check (FBI fingerprint check) portion of the required background investigation.

b. Interim PIV eligibility determinations are temporary and will be recorded in OPM's Central Verification system (CVS), or successor database. Instructions for recording interim PIV eligibility in CVS will be provided in separate guidance.

c. Because the interim PIV eligibility issued under this option is based on a fingerprint check, D/As must manage this risk by putting adequate procedures in place to monitor the completion of the investigation and its prompt adjudication.

d. **Step 2.** ***Final PIV eligibility determination*****:** The procedures outlined under Option 2 (below) for adjudication of the completed investigation apply. If the final credentialing decision is unfavorable, the D/A will record the unfavorable determination in CVS or any successor database, while also taking steps to recover the PIV Credential and render it physically inoperable. Option 2 applies to all final PIV eligibility determinations.

2. **Option 2:** Final PIV eligibility determination (**One-Step Process**)

a. This option must be followed when the D/A decides not to onboard the individual until completion and favorable adjudication of the prerequisite investigation. Under this process the individual will not have access to D/A's physical space or information systems until the investigative and adjudicative processes are complete.

b. Once the investigation is completed, the D/A will make the corresponding

[9] This review must be conducted using the Final Credentialing Standards or successor standards. *See* July 31, 2008 Memorandum from OPM Director, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12* and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, of March 2, 2016, until aligned adjudicative standards are issued in conjunction with the Trusted Workforce 2.0 initiative.
[10] Standard Form (SF) 85, SF 85P, or SF 86 or subsequent forms.
[11] This review must be conducted using the Final Credentialing Standards or successor standards. *See* July 31, 2008 Memorandum from OPM Director, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12* and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, of March 2, 2016, until aligned adjudicative standards are issued in conjunction with the Trusted Workforce 2.0 initiative.

adjudicative decision as required (e.g., credentialing, suitability under CFR 731 (or equivalent standards), and/or national security eligibility under Security Executive Agent Directives (SEAD)). Once the adjudication is made, including the credentialing eligibility determination, the D/A must complete the identity source verification requirements described in option 1.a.i above and proceed with card issuance process.

i. If the D/A makes a favorable determination of suitability/fitness for appointment under 5 CFR part 731 or equivalent standards, or national security eligibility under SEAD, this will result in a favorable PIV eligibility determination. No further credentialing adjudicative action is necessary.

ii. If the D/A is unable to make a favorable national security eligibility determination and decides to place the individual in a non-sensitive position, the D/A will make a credentialing eligibility determination by applying the *credentialing standards*.

iii. When neither a suitability/fitness determination under 5 CFR 731 or equivalent standards nor a national security eligibility determination is required and the D/A decides to place the individual in a non-sensitive position, the D/A will make a credentialing eligibility determination by applying the *credentialing standards*.

c. D/As must ensure that PIV eligibility determinations (favorable or unfavorable) are recorded immediately in CVS. Separate detailed guidance for recording determinations of eligibility for a PIV credential in CVS will be provided.

Credentialing Process for Non-U.S. Nationals

Due to limitations in an ISP's ability to collect background investigation information in locations outside the United States, special investigative considerations apply when a PIV credential is needed for a non-U.S. national in either U.S. based locations or foreign locations. Refer to Appendix A, Credentialing Eligibility of Non-United States Nationals, for additional instructions.

Reciprocity of PIV Eligibility Determinations

1. For the purpose of PIV eligibility determinations, agencies shall not re-investigate or re-adjudicate individuals visiting or temporarily or permanently transferring from another D/A provided a final favorable PIV eligibility determination exists based on an investigation that is at an appropriate tier for the new position.[12]

2. Agencies must exercise reciprocity and accept previous PIV eligibility determinations under the following conditions:

a. The PIV eligibility determination was a favorably adjudicated final (not interim)

[12] Federal Investigative Standards issued by the Security Executive Agent and the Suitability and Credentialing Executive Agent.

determination[13] at the appropriate tier for the new position based on a completed Tier 1 or equivalent or higher level of investigation;

b. There has been no break in service (or in a contractor's association with Government contract work) exceeding 24 months following the favorable adjudication of the previously conducted investigation; and

c. The gaining D/A is not in possession of any new information that calls into question the person's eligibility for a PIV credential.

3. Agencies must consult OPM's CVS, or any successor system, to determine the credentialing status of any prospective employee or contractor in order to determine eligibility for reciprocity.

4. For reciprocity in the case of non-U.S. nationals, see Appendix A, Credentialing of Non-United States Nationals.

Standards and Procedures for Suspending PIV Eligibility

1. When a D/A becomes aware of any credible adverse information that a person may pose an unacceptable risk (to the life, safety, property, or health of employees, contractors, vendors or visitors to a Federal facility; to the Government's physical assets or information systems; to records, including privileged, proprietary, financial or medical records; or to the privacy of the individuals whose data the Government holds in its systems), the D/A's identified responsible decision maker must first assess the nature of the risk.

2. D/As must refer credible adverse information for other action as necessary and appropriate and in a timely manner. Appropriate referrals could be to local law enforcement, an insider threat office, a physical security office, a counterintelligence office, or the FBI, depending on the circumstances, and as consistent with D/A insider threat referral policies.

3. *Required Action for Imminent or Immediate Risk or Danger*. When information is received that suggests, in the decision maker's judgment, that the person presents an imminent risk to facilities or information systems or a danger to the occupants and visitors to a facility or to the public, the D/A must take immediate action to remove the PIV credential from the credential holder's possession if the nature of the risk permits. Additionally, the D/A authorities must suspend or revoke[14] the technical features of the credential that enable access to facilities and information systems and deny the individual access to facilities and information systems until resolution of the issue.

a. The following examples describing information about a covered individual derived from self-reporting or third-party reporting may warrant immediate suspension of credentials. They are provided for illustrative purposes and are not intended to be exhaustive. They

[13] A favorable suitability or national security determination recorded in CVS suffices as a favorable credentialing determination for reciprocity purposes.

[14] If a card suspension mechanism is not available the D/A must revoke the credential following existing NIST standards, FIPS 201-2 or subsequent issuance.

do not replace a D/A decision maker's measured judgment and consideration of all circumstances surrounding the issue.

i. Known or reasonable suspicion of terrorist activities or involvement.
ii. Known or reasonable suspicion of activities demonstrating that the individual has used or intends to use his or her PIV credential or credential tokens to permit access to a Government facility or information system to do harm or permit others to do harm to the facility, its occupants, or its systems.
iii. Known activities, or reasonable suspicion or threat of activities, designed to corrupt, destroy, or otherwise affect the operating status and availability of critical Government information systems.
iv. Gaining, attempting to gain, or assisting others in their efforts 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 with intent to compromise the information, commit identity fraud, or to otherwise use the information in a malicious or harmful way.
v. Violent actions or the threat of violent actions at a Federal workplace.
vi. Bringing, or attempting to bring, an unauthorized weapon into a Federal workplace.
vii. The covered individual's expression of his or her intent to harm or kill him or herself or others.
viii. The covered individual's behavior or statements that allow a reasonable inference that he or she intends to harm him or herself or others.

4. *Investigation of Issues*. As applicable, the covered individual is placed on a paid non-duty status, such as administrative or investigative leave[15] while potential conduct issues of a serious nature are fully investigated.

5. *Discretionary Action when there is No Indication that the Risk is Imminent*. When the D/A decision maker does not judge the risk to be imminent, but finds there is a reasonable basis to believe there may be an unacceptable risk due to issues that potentially impact the individual's eligibility for a PIV credential[16], the D/A decision maker has discretion to determine if the PIV credential and all associated technical features enabling access to facilities and information systems should be suspended or if the individual should retain access until the matter is fully resolved.

6. *Suspension/Revocation of Credential Process*[17]. Derogatory information that results in the suspension of PIV eligibility must also result in the appropriate suspension (or if suspension is not available, the revocation) of the access to physical facilities, information systems, and/or any Derived[18] PIV Credential on the PIV card.

---

[15] Per the Administrative Leave Act of 2016, enacted under section 1138 of the National Defense Authorization Act for Fiscal Year 2017, (Pub. L. 114-328, 130 Stat. 2000, December 23, 2016)
[16] *See* July 31, 2008 Memorandum from OPM Director, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12* and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing Personal Identity Verification (PIV) Credentials and Suspension Mechanism*, of March 2, 2016, or any successor standards.
[17] Follow NIST guidance for implementation of the technical aspects of PIV specific certificate suspension or guidance provided by respective authorized PIV card issuer.
[18] *See* NIST Special Publication 800-57 Guidelines for Derived PIV Credentials, December 2014.

a. When possible and advisable, the D/A should review all available information, including, but not limited to the PIV credential holder's explanation, before deciding to suspend (or revoke) the PIV credential. However, there is no requirement to do so if, in the D/A's judgment, delays created by this review would increase risk. The D/A should err on the side of caution and safety and suspend or revoke the PIV credential if it receives credible information that there is an imminent risk or danger.

b. D/As must have procedures in place to issue emergency notifications when imminent risk calls for immediate suspension or revocation[19].

c. The suspension or revocation steps are particularly important if the credential cannot be safely recovered from the credential holder. D/As must collaborate with their respective Identity, Credential, and Access Management (ICAM) and physical access control systems owners to establish suspension or revocation protocols for circumstances when a PIV credential eligibility is to be suspended. The protocols must be designed to effectuate an immediate suspension or revocation of the card's functionalities (to include physical, logical and derived accesses). Should D/As not be able to suspend the credential certificates, they must revoke the PIV card following NIST guidelines.[20]

Regardless of the means used to suspend or revoke the PIV card D/As must do the following:

a. Whenever possible, collect and secure the PIV credential. This shall be done following the D/A policy and procedures for PIV storage, and in a manner that provides accountability and safeguarding from misuse.

b. Immediately alert all access points at the sponsoring Federal facility (and any other facilities where the individual has been granted access) that the PIV credential and credential tokens have been suspended; provide a physical description or picture of the person when there may be an imminent risk or safety concern, if possible.

c. Terminate any existing access privileges to IT systems, and applications.

d. Report the individual's PIV credential eligibility as "suspended" in CVS (or successor data system).

e. As appropriate, notify and coordinate with agency Insider Threat Programs and/or Federal and local law enforcement offices through established channels. When in doubt, report.[21]

f. The derogatory information that resulted in suspension of the credential is reportable

[19] Per FIPS 201-2 revocation procedures shall at a minimum be completed within 18 hours of notification of issues.
[20] Ibid.
[21] Agencies must have policies in place, such as standard operating procedures and system of record notices under the Privacy Act with law enforcement routine uses, so that required reporting is not unnecessarily delayed.

for national security eligibility[22] or counterintelligence reasons as follows:

i. If the person in question occupies a sensitive position, notify the office within the D/A which is responsible for determining national security eligibility, as appropriate, as well as the office within the D/A responsible for insider threat assessment.
ii. If the person in question occupies a non-sensitive position, the underlying derogatory information will dictate whether D/A counterintelligence and/or insider threat authorities should be notified.

g. For Federal employees who will be unable to perform work while the PIV credential and credential tokens are suspended (and especially when the risk or danger is imminent), the D/A may need to initially place the individual in a paid non-duty status, such as administrative or investigative leave. The D/A should consult with its human resources staff and/or general counsel before taking action. After doing so, the D/A should follow the appropriate procedural requirements to pursue any other action(s) deemed appropriate, such as an adverse action.

h. Whether or not there are appeal rights, and what form they will take, will depend upon the authority under which the action is taken. For instance, if the D/A proposes to take an adverse action against a tenured Federal employee, the procedural requirements in 5 U.S.C. Chapter 75 and OPM's implementing regulations at 5 CFR Part 752 would apply, and an outcome adverse to the employee could be appealed to the Merit Systems Protection Board and, eventually, its reviewing courts, as applicable. For bargaining unit Federal employees, collective bargaining agreements may set forth grievance rights, so close coordination with employee relations staff and D/A counsel is essential.

i. D/A suspending PIV eligibility of contractors shall notify the contracting company of the suspension following appropriate D/A internal requirements.

7. To effectively implement these credentialing standards procedures, D/A must remain vigilant and be prepared to act upon any information that suggests that continued access to facilities and/or information systems poses an unacceptable risk. The comprehensive actions necessary to respond to threats and minimize risk require planning and coordination with human resources, security, counterintelligence, chief information office and insider threat programs. D/A must include PIV eligibility suspension procedures in threat response planning.

Unfavorable Determinations

1. D/As will make unfavorable PIV eligibility determinations as appropriate, following procedures provided in this section.

[22] *See* Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position* (2017).

2. When a D/A makes an unfavorable suitability/fitness and/or national security determination[23] resulting in the loss of employment, the need for PIV eligibility is eliminated. In these cases, the D/A will not make a separate credentialing adjudication. The D/A will document the unfavorable suitability/fitness and/or national security determination[24] and will also document CVS[25] or any successor system to reflect the elimination of PIV eligibility.

3. Agencies must adopt effective procedures to communicate and implement unfavorable PIV eligibility determinations. For cases where the adjudicative process results in an unfavorable credentialing determination, those procedures must include the following[26]:

a. Furnish the individual a comprehensive written explanation of the basis for the denial or revocation of PIV eligibility to the degree that the national security interests of the United States and other applicable law permits.

b. Afford the individual a response opportunity (oral or written) and 30 days to provide information or documentation that may refute or alleviate the concerns.

c. Evaluate the individual's response, and, if the concerns are not eliminated or adequately addressed, notify the individual in writing of the final unfavorable determination and apprise the individual of the appeals process.

d. If applicable, report unfavorable PIV eligibility determinations to the contract entity that employs or seeks to employ the covered individual. While it is appropriate for the D/A to advise the contractor that an unfavorable PIV eligibility determination has been made, it may not be appropriate to disclose additional information about the basis for the determination.[27]

e. The derogatory information that resulted in the unfavorable PIV eligibility determination may also be reportable for national security eligibility or counterintelligence reasons.[28]

---

[23] The appeal process relevant to the underlying suitability and or security determination takes precedence and will apply.

[24] Federal Investigations Notice No. 10-04 dated March 18, 2010 (https://www.dcsa.mil/Portals/91/Documents/pv/GovHRSec/FINs/FY10/fin-10-04.pdf)

[25] 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)

[26] This requirement supersedes the guidance in the 2008 Credentialing Standards.

[27] The Government does not have an employment relationship with individuals performing services under contract, and the Government's interest in making a credentialing determination is limited to its assessment of risk to federally-controlled facilities and information systems. A determination about an individual's ability to work on a Government contract does not necessarily imply that he or she cannot work for the same private employer in some other capacity. Agencies should consult with their legal counsel in considering how to convey unfavorable determinations to the contractor. *See* OPM, Contractor Fitness Adjudication – Best Practices (2013), *at* https://chcoc.gov/content/contractor-fitness-adjudication-%E2%80%93-best-practices. *See also* OPM, Federal Investigations Notice No. 10-05 (2010), *at* (*https://www.dcsa.mil/Portals/91/Documents/pv/GovHRSec/FINs/FY10/fin-10-05.pdf*) (instructing contractors that in taking any actions based on an agency's credentialing decision, they must adhere to their nondiscrimination obligations).

[28] *See* Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or who hold a Sensitive Position* (2017).

Notify the office within the D/A which is responsible for determining national security eligibility, as appropriate.

4. **Individuals found ineligible for a PIV under the Credentialing Standards may not access the federally-controlled facilities and information systems for which a PIV is required and may not be issued an alternate PIV for these purposes.**

5. When an unfavorable PIV eligibility determination is made, the D/A should evaluate the circumstances surrounding the ineligibility for a PIV credential and take a personnel action, if appropriate (with any applicable appeal rights).[29] In the case of an individual employed in the Federal civil service, the grounds for finding the person ineligible may also constitute grounds for pursuing an adverse action (such as removal) to promote the efficiency of the service, or to terminate an appointee who has not yet accrued adverse action rights.

a. In all cases, as soon as PIV credential access is no longer needed, access shall be withdrawn for the PIV credential and any pertinent systems and data bases must be updated to revoke PIV credential tokens and terminate access.

b. Any facility or system access previously granted must be immediately withdrawn for the PIV credential and any data bases showing current PIV credential eligibility must be immediately updated, to include CVS.

6. D/As must have effective procedures in place between personnel security offices, human resource offices, contracting offices, etc., to enable them to work together to address issues or changes that may affect PIV eligibility. For instance, communication between internal D/A offices is essential to ensure an individual does not inappropriately retain physical or logical access when he or she has been subject to unfavorable administrative action (such as when a contractor is removed from the contract) or adverse action (such as when an employee is suspended or removed for conduct reasons). Similarly, communication between D/As is essential. Consult CVS or any successor system to identify D/As that may have a current affiliation with the individual.

7. Agencies are reminded that derogatory information affecting PIV credential eligibility may be reportable under the minimum standards and guidelines for insider threat reporting under E.O. 13587.

8. If the PIV credential cannot be collected and destroyed, then the certification authority (CA) shall be informed and the certificates corresponding to the PIV Authentication key and asymmetric Credential Authentication key on the PIV Credential shall be revoked. If present, the certificates corresponding to the digital signature key and the key management key shall also be revoked.

[29] The denial or revocation of a credential for military members or other persons accompanying United States Forces must be accomplished considering Geneva Convention requirements in accordance with DoD Instruction 5200.46.

Appeals Process[30]

1. D/As must establish an appeals process to review requests by persons who have been determined to be ineligible for a PIV.[31]

2. The appeals process must:

   a. Establish a mechanism for designating a decision-maker or decision-makers on appeal. Any individual who serves as a decision-maker must be different from the individual who made the initial decision to deny or revoke the PIV eligibility. In addition, any individual who serves as an appeal decision-maker must be a Federal employee or military member, since this is an inherently governmental function.

   b. Afford the individual 30 days to provide information (oral or written) that may refute or alleviate the concerns.

   c. Notify the individual in writing of the results of the appeal determination, that the appeals process is final and there is no further right of D/A review.

Further Information

For additional information or if you have questions about this document, please contact the Credentialing Program Office, at 202-606-8460 or via email to CredEA@opm.gov.

Attachments:
Appendix A - Credentialing Eligibility of Non-United States Nationals

[30] Nothing in this section will prohibit the D/A Head from exercising decision authority when the D/A Head certifies that these procedures cannot be made available in a particular case without damaging the national security interests of the United States. This certification shall be conclusive.

[31] There is no right to appeal the PIV Credential "elimination" if the agency's unfavorable suitability, fitness, or national security eligibility determination collaterally results in the loss of employment and the related loss (or *elimination* of need for) of the PIV Credential, or if the PIV is no longer needed because of voluntary or involuntary loss of employment (due to reasons unassociated with existing credentialing criteria). In these cases, PIV eligibility is recorded as "eliminated" in CVS and the PIV credential is withdrawn.

Appendix A

Credentialing Eligibility of Non-United States Nationals

D/As are required to apply the credentialing standards procedures in this issuance to non-U.S. nationals[32] who work as employees or contractors for Federal departments or agencies or others who require long-term logical or physical access to Federal government facilities whether overseas or in the United States.

Due to limitations that apply to the employment of non-U.S. nationals and the ability to collect background investigation information in locations outside the United States, special considerations apply when a PIV credential is needed for a non-U.S. national in either U.S-based locations or foreign locations. In many circumstances investigative standards cannot be met and therefore a PIV may not be issued. Agencies may elect to issue alternative identity credentials in these cases if they wish to accept the risk. Reciprocity rules do NOT apply to D/A issued alternative identity credentials.

The special considerations that apply to the requirements for non-U.S. nationals are outlined below:

Employment Authorization Verification

Location	**Employment Authorization Verification Requirements for Non-U.S. National Federal Employees or Contractors**
U.S. Based Locations	Verify employment eligibility through E-Verify.
U.S. Territories (Other than American Samoa)[33]	Verify immigration status through the USCIS' Systematic Alien Verification for Entitlements (SAVE) system.)[34]
Foreign Locations	n/a

[32] The term "United States national" includes both U.S. citizens and U.S. non-citizen nationals (i.e. American Samoans).

[33] The U.S. territory of American Samoa is not included in the "United States" as defined by the Immigration and Nationality Act, and therefore the DHS E-Verify and SAVE verification programs are unable to verify work authorization or immigration status of individuals in American Samoa. Agencies should conduct such background investigation as may be possible and appropriate under the circumstances in this territory. Prior to 2008, the Commonwealth of the Northern Mariana Islands (CNMI) was also not included in the "United States"; however, on May 8, 2008, the Consolidated Natural Resources Act extended most provisions of the U.S. Immigration Law to the CNMI. The transition of U.S Immigration Law in the CNMI began on November 28, 2009 and was scheduled to end on December 31, 2019. DHS E-Verify may now be available for employment authorization verification in CNMI.

[34] https://www.uscis.gov/save

Appendix A (continuation)

Background Investigation

Location	If the person has been in the U.S. or U.S. Territory for:	Investigation Requirements and Exceptions
U.S. Based Locations or U.S. Territories	3 or more years, **continuously and immediately preceding** the start of Federal affiliation	Initiate the Tier 1 investigation or equivalent after employment authorization or immigration status is verified.
U.S. Based Locations or U.S. Territories	Less than 3 continuous years preceding the start of Federal affiliation	A Tier 1 investigation may NOT be requested on Non-U.S. Nationals in the U.S. or U.S. Territory for less than 3 years. At the discretion of the agency, based on a risk determination, an alternative facility access identity card[35] may be issued until the employee or contractor in question has resided for 3 years in the U.S. or U.S. Territory. If an alternative facility access identity card is issued, the following checks are still required[36]: o FBI fingerprint based National Criminal History Check (NCHC) must be completed before an alternative facility access identity card is issued o FBI Investigations files (Name Check) o Name check against the Terrorist Screening database o USCIS Check against SAVE o Any additional checks the agency determines are necessary (agency discretion) The above checks will provide limited results, will not constitute a Tier 1 investigation and will not be documented as a Tier 1 investigation.
Foreign Locations	N/A	It is generally not possible to conduct a Tier 1 investigation on a Non-U.S. National in a foreign location. (Exceptions are possible for Non-U.S. Nationals who have resided in the U.S. or U.S. Territory for 3 years prior to the conduct of a Tier 1 investigation.) If an investigation that is equivalent to a Tier 1 investigation cannot be performed, an alternative facility access identity card may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander, and/or other agency official, as appropriate, based on a risk determination.

[35] Reciprocity rules do NOT apply to agency issued alternative facility access identity cards.
[36] Agencies may establish a Special Agreement Check (SAC) with DCSA for the purpose of conducting these checks on non-U.S. Nationals. Contact DCSA Customer Liaison at 724-794-5612.