CMS SECURITY Information

CMS specific information in support of the CMS Security terms and conditions (June 2026), FAR 52.204-9, HHSAR 352.204-71 and HHSAR 352.204-73. Questions regarding the information and guidance provided should be directed to your assigned Contracting Officer Representative (COR).

1. SCREENING OF CONTRACTOR EMPLOYEES

ii. Vetting and Credentialing Application Process (Identity and Credentialling Tool (ICT) Application)

i. **Vetting and Credential Sponsor**: The COR will review and approve or deny the ICT application before the forms are submitted to the CMS, Office of Security, Facilities & Logistics Operations (OSFLO), Security Management Group (SMG), Division of Credentialing Operations (DCO) for processing. **Suitability Requirements:** In accordance with 5 CFR 731.202 (Criteria for Making Suitability Determinations) and HHSAR 352.204-73(d), CMS reserves the right to decline access to contractor employees. The following (non-exclusive) list provides examples of reasons why contractor employees may be declined access:

   i. Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;
   ii. Falsification of information entered on forms or of other documents submitted;
   iii. Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and
   iv. Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

ii. **Contractor Application Required Submissions:** Unless otherwise directed by the COR or CMS/OSFLO, Applicants are required to electronically submit their application via CMS's Identity and Credentialing Tool. To assist users with the application process, a user's guide is located at: https://www.cms.gov/about-cms/work-us/business-resources/information-current-cms-contract-holders/contractor-information/training The user's guide link should be used to obtain the most current instructional guidance and required forms as amended by the CMS Security Office.

   i. **Declaration for Federal Employment Form (OF-306):** Contractor employees shall complete an OF-306 during the electronic application process.
   ii. **Resume: Contractor** employees shall upload their resume during the electronic application process. No specific format is required.

iii. **Drug Free Workplace Policy (DFWP)**: Contractor employees shall read the Division of Personnel Security (DPS) Drug Free Workplace Acknowledgement (DFWA) document. If the Contractor employee agrees to adhere to the current Federal workplace drug free policy, they shall concur by signing, dating, and uploading the DFWA document within the electronic application.

iv. **Seasonal Employees:** If you have seasonal employees (will be on the contract for less than 6 months total), you must contact the COR for more detailed information on the vetting process for those individuals. **PIV Applicant Training:** Contractor employees needing a PIV Credential shall complete the HHS PIV Applicant Training, which is found at: https://www.cms.gov/about-cms/work-us/business-resources/information-current-cms-contract-holders/contractor-information/training. A copy of the completion certificate shall be included with the electronic application.

iii. CMS Applicant Evaluations: CMS will evaluate an Applicant's required access level. Part of this evaluation may also include whether an applicant is eligible for reciprocity. Once the review is complete and accepted for further processing, the Applicant will be contacted by CMS/OSFLO to submit the information below, as applicable.

i. **NBIS e-APP:** Contractor employees will be required to submit information into the National Background Investigation Services (NBIS) Electronic Application (e-APP), a web-based automated system that is designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness, credentialing and adjudication purposes.

ii. **Fingerprints:**

1. During the investigation process, Contractor employees are required to obtain fingerprints by completing one of the following:

    a. Scheduling an appointment in the CMS Baltimore Badging Office,
    b. Utilizing the Sterling/ID.me Digital Live Scan process, or
    c. Opting to visit an alternate facility (e.g., police station, post office, etc.), receiving fingerprint hard cards, and mailing the completed hard cards back to CMS for processing.

2. Costs associated with fingerprinting shall be applied in accordance with the contract structure and the contractor's disclosed accounting practices.
3. Further instructions for obtaining fingerprints will be provided by CMS/OSFLO.

iii. **Access to Restricted Area(s):** The CMS COR will initiate all PIV Credential holders' physical access requests via the Physical Access Control System (PACS) Central at: https://pam.cms.gov/identify.php

iv. **Vetting and Credential Sponsor**: The CMS Contracting Officer's Representative (COR) will be the Vetting and Credential Sponsor and point of contact for the Contractor's ICT application.

i. **CMS COR Position Designation –** Upon contract award, the CMS COR will complete a position sensitivity and risk designation based on the duties associated with the Contractor employee's position. The risk and sensitivity level designations will be the basis for determining the level and type of personnel security investigations required for Contractor employees. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably adjudicated. Additionally, the DCSA e-APP and other required forms must be accepted by CMS/OSFLO before logical or physical access can be granted.

PIV Credential Issuance: If identified as requiring a PIV credential, upon approval of the PIV Credential application process and prior to receiving physical or logical access, applicants will be contacted to appear in person to a PIV Card Issuance Facility (PCIF), at least two (2) times (estimated at one hour for each visit), and shall provide two (2) original forms of identity source documents in order to generate the PIV Credential. The identity source documents shall come from the list of acceptable documents included in FIPS 201-3, located at: https://csrc.nist.gov/pubs/fips/201-3/final. At least one (1) document shall be a valid State or Federal government-issued picture ID. For questions, please email the CMS Credentialing Office at Badging@cms.hhs.gov or call (410) 786-1605. All travel costs associated with PIV issuance shall be applied in accordance with the contract structure and the contractor's disclosed accounting practices. As necessary, Contractor's should obtain advanced approval for any travel required.

iii. Background Investigation and Adjudication

a. After contract award and receipt of an ICT application from the Contractor employee, CMS will initiate the agency access procedures to include a background investigation.

b. The Contractor shall ensure contract performance continues through the duration of the vetting and credentialing process.

i. Contractor employees who fail to cooperate with DCSA, a contract background investigator working on behalf of DCSA, or Agency representatives during the background investigation process will be required to cease working on the contract immediately.

ii. CMS/OSFLO may provide written notification to the Contractor employee, with a copy to the COR, of all suitability/non-suitability decisions. A CMS adjudicative decision (based on criminal history

results or completed investigation results) for a contractor employee is final and is not subject to appeal.

iii. The Contractor shall immediately submit an adverse information report, in writing to the CO with a copy to the COR, of any adverse information regarding any of its employees that may impact their ability to perform under this contract. Reports should be based on reliable and substantiated information, not on rumor or innuendo. The report shall include, at a minimum, the Contractor employee's name and associated contract number along with the adverse information. The COR will forward the adverse information report to CMS/OSFLO for review and action to personnelsecurity@cms.hhs.gov.

1. Examples of "adverse information" include but are not limited to the following: foreign activities, media contact, arrests, criminal conduct, financial anomalies, alcohol/drug related treatment, etc. (cf. 5 CFR 731.202(b), Criteria for Making Suitability Determinations).

iv. Under the Privacy Act of 1974, Contractor employees may request a copy of their own investigation by submitting a written request to the DCSA Federal Investigative Services (FIS) Freedom of Information (FOI) office, Form INV 100, NOV 2023. https://www.dcsa.mil/Contact-Us/Privacy-Civil-Liberties-FOIA/bir/

iv. Background Investigation

a. Contract Renewal: If a Contractor employee remains on the renewed contract, the Contractor employee shall complete and submit a new ICT application (existing user renewal request) and all other required documents (i.e., signed and dated within 12 months), The COR shall review the renewal request. Foreign Nationals shall also submit current work authorization documents (i.e., I-797 or I-94, permanent resident card, visa, etc.).

v. Identification Card Custody and Control

a. The Contractor is responsible for the custody and control of all forms of Federal identification issued by CMS to Contractor employees. The Contractor shall immediately update the roster in the Identity and Credentialing tool (ICT) when a Contractor employee no longer requires agency access due to transfer, completion of a project, retirement, removal from work on the contract, or termination of employment. Return all CMS PIV Credentials to:

The Centers for Medicare and Medicaid Services
Attn: OSFLO/SMG/DCO, Mailstop: SL-17-06
7500 Security Boulevard
Baltimore, Maryland 21244

b. Renewal: A Contractor employee's CMS issued PIV Credential is valid for a maximum of five (5) years and 9 months or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin **six (6) weeks** before the PIV Credential expiration date by contacting the COR.

i. If a PIV is not renewed before it expires, the Contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

PIV credentials also contain certificate(s) that have an expiration date different than the date printed on the card. These certificates require annual updates from the issuance date. The annual updates should be coordinated between the contractor and the COR.

b. **Lost/Stolen:** Immediately upon detection that an PIV Credential is lost or stolen, the Contractor or Contractor employee shall report a lost or stolen PIV Credential to the COR and the Division of Physical Security Operations at SECURITY@cms.hhs.gov. The Contractor shall also submit an Incident Report within 48 hours, to the COR and DCO to Badging@cms.hhs.gov. The Incident Report shall describe the circumstances of the loss or theft. If the loss or theft is reported by the Contractor to the local police, a copy of the police report shall be provided to the COR. The Contractor employee shall sign in daily for facility access and may have limited access to information systems and other resources until the replacement card is issued.

c. **Replacement**: A PIV credential will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than three (3) days, provided there is a continuing need for agency access to perform work under the contract.

vi. Surrender PIV Cards/Access Cards and Government Equipment

a. Upon notification that routine access to CMS facilities, sensitive information, federally controlled information systems or other CMS resources is no longer required, the Contractor shall surrender the CMS issued ID card, access card, keys, computer equipment, and other government property to the CMS COR. Contractor employees who do not return their government issued property within **48 hours** of the last day of authorized access to CMS may be permanently barred from CMS systems and facilities and may be subject to fines and penalties, as authorized by applicable Federal or State laws.

vii. Mandatory Trainings

a. All contractors are required to take Security & Privacy training as indicated by CMS. Various systems may require additional training.

2. POINTS OF CONTACT

i. For questions regarding the above information or the badging process, please contact your COR or contact the CMS Baltimore Credentialing Office at Badging@cms.hhs.gov or (410) 786-1605.

ii. For questions related to lost or stolen PIV cards, please contact your COR and/or SECURITY@cms.hhs.gov.

For questions related to the Agency Vetting and Credentialing program contact vandc_hspd12@cms.hhs.gov

For questions related to Restricted Logical Access (RLA) tokens contact the CMS IT help desk at 410-786-2580.