CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-20 One-Time Notification	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 1674	**Date: June 17, 2016**
	Change Request 9645

SUBJECT: Medicare Administrative Contractors (MACs) Analysis of the Proposed Contract CMS Security Clause Update

I. SUMMARY OF CHANGES: Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors has directed that agencies expedite the full use of the Personal Identity Verification (PIV) credentials for access to federal facilities and information systems. The Department of Health and Human Services (HHS) outlined a set of requirements that needs to be included in the Centers for Medicare & Medicaid Services (CMS) implementation policy, in order for that policy to be effective in achieving the goals of HSPD-12 and realizing the full benefits of PIV credentials. Based on updated direction from HHS and CMS, this initiative is moving further towards the implementation of PIV and PIV-I (Personal Identity Verification Interoperability). As a result, the Office of Acquisition and Grants Management (OAGM) has developed draft contract language in support of the HSPD-12 initiative.

The purpose of this Change Request (CR) is to have the MACs perform an analysis regarding the attached draft OAGM contract language to evaluate cost and operational impacts, and to provide a Rough Order of Magnitude (ROM) to CMS for planning purposes only. As part of this process for considering implementing HSPD-12, the MACs would review the proposed contract language to evaluate the documented requirements to fully determine possible impacts. MACs shall consider the workload associated with the planning, implementation, education and ongoing support required to meet the proposed contract language in their analysis.

EFFECTIVE DATE: July 18, 2016**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: July 18, 2016

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
N/A	N/A

III. FUNDING:

For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically

authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

One Time Notification

Attachment - One-Time Notification

Pub. 100-20	Transmittal: 1674	Date: June 17, 2016	Change Request: 9645

SUBJECT: Medicare Administrative Contractors (MACs) Analysis of the Proposed Contract CMS Security Clause Update

EFFECTIVE DATE: July 18, 2016
**Unless otherwise specified, the effective date is the date of service.*

IMPLEMENTATION DATE: July 18, 2016

I. GENERAL INFORMATION

A. Background: In August 2004, President George W. Bush issued Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors where the Office of Management and Budget (OMB) has directed that agencies expedite the Executive Branch's full use of the PIV credentials for access to federal facilities and information systems. The Department of HHS outlined a set of requirements that needs to be included in the CMS implementation policy, in order for that policy to be effective in achieving the goals of HSPD-12 and realizing the full benefits of PIV credentials. HHS policy states: Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with National Institute of Standards and Technology (NIST) guidelines.

In accordance with a CIO Policy Directive #15-01: Strong Authentication, the MACs have taken the initial step in deploying RSA tokens to provide Multi-Factor Authentication (MFA) to their systems. Based on updated direction from HHS and CMS, this initiative is moving further towards the implementation of PIV and PIV-I (Personal Identity Verification Interoperability). As a result, the Office of Acquisition and Grants Management (OAGM) has developed draft contract language in support of the HSPD-12 initiative.

There are currently two phases defined for the implementation of PIV/PIV-I. Phase 1 will focus on users with access to the CMS.Local Area Network (logging on to the CMS network at the Baltimore Data Center). PIV Cards will be issued to users within 50 miles of CMS or a CMS Regional Office, requiring at least two one hour visits to a CMS location. PIV-I cards will issued to users outside of the 50 mile radius, which will not require a visit to a CMS location.

Phase II will address users with access to resources that reside within the Virtual Data Centers (VDC). For this phase, PIV-I will be exclusively used. Phase II does not include:

- Users with access to resources that reside outside the Virtual Data Centers (HP-VDC & CDS-VDC) and are within boundaries of a CMS FISMA systems;
- Health Plans and Providers;
- States; and,
- Other Federal Agencies.

PIV-I mobile enrollment stations will be made available for environments with a significant number of applicants (approximately 10 or more) that have a location more than 50 miles from CMS or any of its regional offices.

The purpose of this CR is to have the MACs perform an analysis regarding the attached draft OAGM contract language to evaluate cost and operational impacts, and to provide a Rough Order of Magnitude (ROM) to CMS for planning purposes only. As part of this process for considering implementing HSPD-12,

the MACs would review the proposed contract language to evaluate the documented requirements to fully determine possible impacts. This review should include analyzing Phase I and Phase II requirements.

MACs shall consider the workload associated with the planning, implementation, education and ongoing support required to meet the proposed contract language in their analysis.

B. Policy: Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
9645.1	MACs shall perform an analysis to determine effort, costs and operational impacts to implement the requirements described in 9645.1.1 through 9645.1.9. Relationships with any affected subcontractors should be considered/included in the analysis and the impacts to the subcontractor should be identifiable within the analysis.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.1	MACs shall detail the effort and costs with implementing compliant card readers and middleware for logical system access (section a of the proposed contract language). This should consider changes/additions to existing infrastructure and the number of users impacted.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.2	MACs shall evaluate the process for screening employees and detail the effort, costs and operational impacts associated with screening employees (section c of the proposed contract language). This should consider any travel associated expenses, applicant evaluations and issuance of badges.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.3	MACs shall evaluate the cost and effort for post badging training requirements for employees (section e of the proposed contract language).	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.4	MACs shall evaluate the process for background investigation and adjudication (section f of the proposed contract language) to determine process impacts including costs, efforts and operational impacts.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.5	MACs shall provide an analysis of the impacts of the background investigation costs applied to an employee that leaves or is no longer associated with the contractor within one year (section g of the proposed contract language).	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.6	MACs shall evaluate the custody and surrender of Federal Identification (access card) to determine costs,	X	X	X	X					CEDI, RRB, RRB-SMAC

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	efforts and operational impacts associated (sections h and i of the proposed contract language).									
9645.1.7	MACs shall provide the impacts for any other items (adverse or otherwise) they deem appropriate or not covered above as they affect the costs, efforts and operational impacts associated with implementing PIV credentialing to meet the proposed contract language.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.8	MACs shall provide a Rough Order of Magnitude (ROM) to CMS (for planning purposes only) that details all projected costs determined by their analysis associated with meeting the proposed contract language, including detailing requirements for Phase I and II of the PIV/PIV-I deployment.	X	X	X	X					CEDI, RRB, RRB-SMAC
9645.1.9	Upon completion of the anlaysis of the proposed contract language, the Rough Order of Magnitude (ROM) that details the costs, efforts and operational impacts of implementing the new contract language should be delivered to Frank Schreibman, Frank.Schreibman@cms.hhs.gov). A template for a ROM has been attached that should be used to document the analysis results.	X	X	X	X					CEDI, RRB, RRB-SMAC

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			DME MAC	CEDI
		A	B	HHH		
	None					

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A
"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Frank Schreibman, 410-786-0336 or frank.schreibman@cms.hhs.gov.

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VI. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 2

CMS SECURITY CLAUSE ANALYSIS ROM
FOR PLANNING PURPOSES ONLY

Please consider and include details of all costs and operational impacts for relationships with any affected subcontractors.

Section 1

MACs shall detail the effort and costs with implementing compliant card readers and middleware for logical system access (section a of the proposed contract language). This should consider changes/additions to existing infrastructure and the number of users impacted.
Description of Level of Effort:
Additional Equipment Needed:
Changes Required to Infrastructure (if any):
Number of Users Impacted:
Associated Costs:

Section 2

MACs shall evaluate the process for screening employees and detail the effort, costs and operational impacts associated with screening employees (section c of the proposed contract language). This should consider any travel associated expenses, applicant evaluations and issuance of badges.
Description of Level of Effort:
Changes Required to Employee Screening Processes (if any):
Additional Training Necessary:
Associated Costs:

Section 3

MACs shall evaluate the cost and effort for post badging training requirements for employees (section e of the proposed contract language).
Description of Level of Effort:
Changes Required to Post Badging Training Processes (if any):
Associated Costs:

Section 4

MACs shall evaluate the process for background investigation and adjudication (section f of the proposed contract language) to determine process impacts including costs, efforts and operational impacts.
Description of Level of Effort:
Changes Required to Background Investigation Process (if any):
Associated Costs:

Section 5

MACs shall provide an analysis of the impacts of the background investigation costs applied to an employee that leaves or is no longer associated with the contractor within one year (section g of the proposed contract language).
Description of Level of Effort:
Impacts of Employee Leaving:
Associated Costs:

Section 6

MACs shall evaluate the custody and surrender of Federal Identification (access card) to determine costs, efforts and operational impacts associated (sections h and i of the proposed contract language).
Description of Level of Effort:
Impact of Custody Responsibilities for Federal Identification:
Associated Costs:

Section 7

MACs shall provide the impacts for any other items (adverse or otherwise) they deem appropriate or not covered above as they affect the costs, efforts and operational impacts associated with implementing PIV credentialing to meet the proposed contract language.

Other Impacts or Items to Consider:

Description of Level of Effort:

Associated Costs:

Section 8

Please provide overall costs as a result of addressing sections 1 through 8 above. Additionally, please provide any additional discussion you feel is pertinent to this effort.

Total Associated Costs:

Other Discussion:

CMS SECURITY CLAUSE

<The contracting officer shall insert the following language for all new solicitations issued after April xx, 2016 and resultant contracts; and, contracts that require physical access to CMS facilities and/or access to CMS Federally Controlled Information Systems as defined by OMB Memo M-05-24.
**NOTE: CMS has many versions and variations of a CMS Security Clause in existing contracts. Incorporate this language in your contract if no other credentialing language is currently in your contract. At the request of OTS and OEI, DQAT will be instructing that various contracts be updated with consideration given to the Federal Information Systems accessible by the contractor.*

IMPORTANT: *Please also remember to include FAR Clauses*

- *FAR 52.204-9 – Personal Identity Verification of Contractor Personnel*
- *FAR 52.222-54 – Employment Eligibility Verification*

Note: The reference to section H does not need to be included if UCF is not being utilized. Further, delete all blue text instructions and ensure any yellow highlighted information is complete in the final version of the provision/clause.>

H.x CMS SECURITY CLAUSE

a. Applicability

In accordance with OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004, and Federal Information Processing Standard (FIPS) PUB Number 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, CMS must achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and/or logical access to federally controlled information systems. Contractors that require routine physical access to a CMS facility and/or routine access to a CMS federally controlled information system will be required to obtain a CMS issued PIV, PIV-I or Locally Based Physical Access card. FIPS PUB 201-2 specifies the architecture and technical requirements for a common identification standard for Federal employees and Contractors.

When a PIV or PIV-I card is provided, it shall be used in conjunction with a compliant card reader and middleware for logical system access. The Contractor shall (1) Include FIPS 201-2 compliant, HSPD-12 card readers with the purchase of servers, desktops, and laptops; and (2) comply with FAR 52.204-9, Personal Identity Verification of Contractor Personnel.

b. Definitions

"Agency Access" means access to CMS facilities, sensitive information, information systems or other CMS resources.

"Applicant" is a Contractor employee for whom the Contractor submits an application for a CMS identification card.

"Contractor Employee" means prime Contractor and subcontractor employees who require agency access to perform work under a CMS contract.

"Official station"— As defined by Federal Travel Regulations, An area defined by the agency that includes the location where the employee regularly performs his or her duties or an invitational traveler's home or regular place of business. The area may be a mileage radius around a particular point, a geographic boundary, or any other definite domain, provided no part of the area is more than 50 miles from where the employee regularly performs his or her duties or from an invitational traveler's home or

regular place of business. If the employee's work involves recurring travel or varies on a recurring basis, the location where the work activities of the employee's position of record are based is considered the regular place of work.

"Federal Identification Card" (or "ID card") means a federal government issued or accepted identification card such as a Personal Identity Verification (PIV) card, Personal Identity Verification-Interoperable (PIV-I) card, or a Local-Based Physical Access Card issued by CMS, or a Local-Based Physical Access Card issued by another Federal agency and approved by CMS. "Issuing Office" means the CMS entity that issues identification cards to Contractor employees.

"Locally Based Physical Access Card" means an access Card that is graphically personalized for visual identification, that does not contain an embedded computer chip, and is only used for physical access.

"Local Security Servicing Organization" means the CMS entity that provides security services to the CMS organization sponsoring the contract, Division of Physical Security and Strategic Information (DPSSI).

"Logical Access" means the ability for the Contractor to interact with CMS information systems, databases, digital infrastructure, or data via access control procedures such as identification, authentication, and authorization.

"Personal Identity Verification (PIV) card," as defined in FIPS PUB 201-2, is a physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

"Personal Identity Verification-Interoperable (PIV-I) card" similar to a PIV card, is a physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV-I cards are issued by a non-federal government entity to non-federal government staff. PIV-I cards are issued in a manner that allows federal relying parties to trust the cards. The PIV-I cards uses the same standards of vetting and issuance developed by the U.S. government for its employees

c. Screening of Contractor Employees

i. Contractor Screening of Applicants

1. Contractor Responsibility: The Contractor shall pre-screen individuals designated for employment under any CMS contract by verifying minimum suitability requirements to ensure that only qualified candidates are considered for contract employment. At the discretion of the government, the government reserves the right to request and/or review Contractor employee vetting processes. The federal minimum suitability requirements can be found below in section (c)(2)—Suitability Requirements, and are also contained in 5 CFR 731.202. The Contractor shall exercise due diligence in pre-screening all employees prior to submission to CMS for agency access.

2. Alien Status: The Contractor shall monitor an alien's (foreign nationals) continued authorization for employment in the United States. If requested by the Agency, the Contractor shall provide documentation to the Contracting Officer (CO) or the Contracting Officer's Representative (COR) that validates that the Employment Eligibility Verification (e-Verify) requirement has been met for each Contractor or sub-

Contractor employee working on the contract in accordance with Federal Acquisition Regulation (FAR) 52.222-54 - Employment Eligibility Verification.

3. Residency Requirement: All CMS Contractor applicants shall have lived in the United States at least three (3) out of the last five (5) years prior to submitting an application for a Federal ID Card. CMS will process background investigations for foreign nationals in accordance with Office of Personnel Management (OPM) guidance. Contractor employees who worked for the U. S. Government as an employee overseas in a Federal or military capacity; and/or been a dependent of a U.S. Federal or military employee serving overseas, must be able to provide state-side reference coverage. State-side coverage information is required to make a suitability or security determination. Examples of state-side coverage information include: the state-side address of the company headquarters where the applicant's personnel file is located, the state-side address of the Professor in charge of the applicant's "Study Abroad" program, the religious organization, charity, educational, or other non-profit organization records for the applicant's overseas missions, and/or the state-side addresses of anyone who worked or studied with the applicant while overseas.

4. Selective Service Registration: All males born after December 31, 1959, must meet the Federal Selective Service System requirements as established on www.sss.gov.

ii. Identification Card Application Process

ID Card Sponsor: The CMS Contracting Officer's Representative (COR) will be the CMS ID card Sponsor and point of contact for the Contractor's application for a CMS ID card. The COR will review and approve/deny the HHS ID Badge Request before the form is submitted to the CMS, Office of Support Services and Operations, (OSSO), Division of Personnel Security Services (DPS), for processing. If approved, an applicant may be issued either a Personal Identity Verification (PIV) or PIV- I card that meets the standards of HSPD-12 or a Local-Based Physical Access Card.

Contractor Application Required Submissions: All applicants shall submit an HHS ID Badge Request form for issuance of a Federal ID Card. Unless otherwise directed by the ID Card Sponsor or DPS, applicants are required to electronically submit the request form via CMS' Enterprise User Administration (EUA) Electronic Front-end Interface (EFI) system, which is located at https://eua.cms.gov/efi. To assist users with the application process, a user's guide is located at:https://www.cms.gov/About-CMS/Contracting-With-CMS/ContractingGeneralInformation/Contracting-Policy-and-Resources.html.

The EUA users guide link should be used to obtain the most current instructional guidance.

PIV Training: Contractors who need PIV or PIV-I card shall complete HHS PIV Applicant Training, which is found at https://www.cms.gov/About-CMS/Contracting-With-CMS/ContractingGeneralInformation/Contracting-Policy-and-Resources.html. A copy of the completion certificate shall be included with the EFI application.

CMS Applicant Evaluations: CMS will evaluate an applicant's required access level. Once the review is complete and accepted for further processing, the applicant will be contacted by DPS to submit the below information, as applicable.

1. **e-QIP**: Contractor employees will be required to submit information into e-QIP, 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 and credentialing purposes.
2. **Fingerprints**: Instructions for obtaining fingerprints will be provided by CMS, OSSO, DPS.
3. **OF 306**: Contractor employees may be required to complete the Optional Form (OF) 306, Declaration for Federal Employment which can be found at https://www.opm.gov/forms/pdf_fill/of0306.PDF.

4. **Access to Restricted Area(s)**: The CMS COR will initiate all Federal ID card holders' physical access requests via Physical Access Control System (PACS) Central at https://pam.cms.local.

Suitability Requirements: CMS may decline to grant agency access to a Contractor employee including, but not limited to, any of the criteria cited below:

1. Misconduct or negligence in employment;
2. Criminal or dishonest conduct;
3. Material, intentional false statement, or deception or fraud in examination or appointment;
4. Refusal to furnish testimony as required by § 5.4 of 5 CFR 731.202;
5. Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;
6. Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;
7. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and
8. Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

Badge Issuance: Upon approval of the badging application process and prior to starting work on the contract, applicants whose official station is located within 50 miles from CMS' central office or one of its regional offices will be contacted to appear in person, at least two times (estimated at one hour for each visit), and shall provide two (2) original forms of identity source documents in order to generate the badge/ID. The identity source documents shall come from the list of acceptable documents included in FIPS 201-2, located at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf. At least one (1) document shall be a valid State or Federal government-issued picture ID. PIV-I mobile enrollment stations will be made available for applicants that have an official station more than 50 miles from CMS or any of its regional offices, and the employee will not need to travel to a CMS Office. The Contractor will be contacted by CMS for further instructions on the badging process in this scenario.

d. CMS Position Designation Assessment

CMS will assign a risk and sensitivity level designation analysis to the overall contract and/or to Contractor employee positions by category, group or individual. 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 OPM e-QIP and other required forms must be accepted by DPS before a CMS identification card will be issued.

e. Post Badging Training Requirements:

Contractor employees that receive an HHS ID Badge are expected to complete the following online trainings each year, according to the timeframes indicated below, and annually thereafter. The below list is not all inclusive and the COR may indicate training that must be taken in addition to the below:

i. **Security and Insider Threat Awareness and Training (30 days after receiving badge):** This course outlines the role of Contractors with regard to protecting information and ensuring the secure operation of CMS federally controlled information systems. Estimated time to complete is one hour.

ii. **Computer Based Training (CBT)** (within 3 days of approved EUA account): This training offers several modules to familiarize contractor employees with features of CMS' webinar service. Estimated time to complete is one hour.

f. Background Investigation and Adjudication

Upon contract award and receipt of an HHS ID Badge Request, CMS will initiate the Agency Access procedures, to include a background investigation.

CMS may accept favorable background investigation adjudications from other Federal agencies when there has been no break in service. A favorable adjudication does not preclude CMS from initiating a new investigation when deemed necessary. Each CMS sponsored Contractor shall use the OPM e-QIP system to complete any required investigative forms.

The Contractor remains fully responsible for ensuring contract performance pending completion of background investigations of Contractor personnel. Employees that do not require access to CMS federally controlled information systems, facilities, or sensitive information in order to perform their duties may begin work on a contract immediately and need not submit an HHS ID Badge Request.

i. Failure to cooperate with OPM or Agency representatives during the background investigation process is considered grounds for removal from the contract.
ii. DPS 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) is final, and is not subject to appeal.
iii. Contractor personnel for whom DPS determines to be ineligible for ID issuance will be required to cease working on the contract immediately.
iv. 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 the DPS for review and/or action.
v. At the Agency's discretion, Contractor personnel may be provided an opportunity to explain or refute unfavorable information before an adjudicative decision is rendered on whether or not to withdraw the Federal ID from the individual in question. Under the provision of the Privacy Act of 1974, Contractor personnel may request a copy of their own investigation by submitting a written request to the OPM Federal Investigative Services (FIS) Freedom of Information (FOI) office. The following OPM-FOI link is being provided to afford one the instructions for obtaining a copy of one's file: https://www.opm.gov/investigations/freedom-of-information-and-privacy-act-requests/.

g. Background Investigation Cost

The government will bear the cost of background investigations that are performed at the direction of CMS' personnel security representatives by the Federal government's approved and designated background investigation service provider, the OPM.

At the Agency's discretion, if an investigated Contractor employee leaves the employment of the Contractor, or otherwise is no longer associated with the contract within one (1) year from the date the background investigation was completed, the Contractor may be required to reimburse CMS for the full cost of the investigation. Depending upon the type of background investigation conducted and the cost incurred by CMS, the Contractor cost will be determined based upon the current OPM fiscal year billing rates, which can be found at http://www.opm.gov/investigations/background-investigations/federal-investigations-notices. The amount to be paid by the Contractor shall be due and payable when the CO submits a written letter notifying the Contractor as to the cost of the investigation. The Contractor shall pay the amount due within thirty (30) days of the date of the CO's letter by check, made payable to the "United States Treasury." The Contractor shall provide a copy of the CO's letter as an attachment to the check and submit both to the Office of Financial Management at the following address:

Centers for Medicare & Medicaid Services
PO Box 7520
Baltimore, Maryland 21207

h. **Identification Card Custody and Control**

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 notify the COR 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 Federal ID cards to:

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

The Contractor shall also ensure that Contractor employees comply with CMS requirements concerning the renewal, loss, theft, or damage of an ID card.

Failure to comply with the requirements for custody and control of CMS issued ID cards may result in a delay in withholding final payment or contract termination, based on the potential for serious harm caused by inappropriate access to CMS facilities, sensitive information, information systems or other CMS resources.

i. **Renewal**: A Contractor employee's CMS issued ID card 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 weeks before the ID card expiration date by contacting the COR. If an ID card 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. Contractor ID card certificate(s) require yearly updates from the issuance date. The yearly updates should be coordinated between the contractor and the COR.

ii. **Lost/Stolen**: Immediately upon detection that an ID card is lost or stolen, the Contractor or Contractor employee shall report a lost or stolen ID card to the COR and the local security servicing organization at SECURITY@cms.hhs.gov. The Contractor shall also submit an Incident Report within 48 hours, to the COR, DPS at Badging@cms.hhs.gov, and the local security servicing organization. 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.

iii. **Replacement**: An ID card 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.

In the event that the PIV card or certificate(s) are not renewed in a timely fashion, or the ID card requires replacement due to being lost, stolen, or damaged, the contractor employee will go through the "Badge Issuance" process again as described in above in section (c)(2). In any of these events, contact your COR to coordinate the appropriate next steps.

i. Surrender ID Cards/Access Cards, Government Equipment

CMS reserves the right to suspend or withdraw ID card access at any time for any reason. Access will be restored upon the resolution of the issue(s).

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 or directly to CMS at the address referenced above in section (f). DPS Contractor personnel 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.