SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 FAR 52.252-1 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

http://www.arnet.gov/far/

H.2 352.237-75 KEY PERSONNEL (DEC 2015)

The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to the contractor voluntarily diverting any of the specified individuals to other programs or contracts the Contractor shall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractor is terminated for cause or separates from the contractor voluntarily with less than thirty days notice, the Contractor shall provide the maximum notice practicable under the circumstances. The Contractor shall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

H.3 POST AWARD BUSINESS ETHICS, CONFLICT OF INTEREST AND COMPLIANCE (OCT 2015)

a. General: It is imperative that the Contractor and the services provided under this contract be free, to the greatest extent possible, of all Organizational and Personal Conflicts of Interest. In this clause, all references to Organizational and/or Personal Conflicts of Interests will be referred to individually or collectively, as the text justifies, as Conflicts of Interest (COI). Except as provided below, the Contracting Officer shall not maintain a contract with a Contractor that the Contracting Officer determines has, or has the potential for, an unresolved COI. However, in accordance with FAR 9.503 Waiver, the Contracting Officer may contract with a Contractor that has an unresolved COI if he/she determines that it is in the best interest of the Government to do so.

b. Definitions:

Actual COI– means that the COI is currently in existence as determined by the Offeror's or Contractor's Compliance Officer and/or as determined by CMS. This form of COI will require avoidance, neutralization or mitigation acceptable to CMS.

Affiliates – As defined in FAR 2.101 means associated business concerns or individual(s) if, directly or indirectly either one controls or can control the other; or a third party controls or can control both.

For purposes of this contract, affiliate control or influence may include, but is not limited to:

(a) Interlocking management or ownership (e.g., individuals serving in similar capacities in several companies);
(b) Identity of interests among family members such as spouse/domestic partner and/or any dependent of the respondent;
(c) Shared facilities and equipment;
(d) Common use of employees; or
(e) A business concern organized just prior to, or immediately following, the release of a solicitation or request for information, which has the same or similar management, ownership, or principal employees as the Offeror or Contractor.

Any business, whether or not it is organized for profit or located in the United States or its outlying areas, or person may be found to be an affiliate. Control may be affirmative or negative and it is immaterial whether it is exercised so long as the power to control exists.

Apparent (Perceived) COI – means that the COI on first observation appears to be an actual or potential COI, but may or may not be after analysis. Even if the apparent COI is determined to be non-existent, this perception may still require further explanation.

Financial Interests/Relationships – means a healthcare related direct or indirect ownership or investment interest (including an option or non-vested interest) in any entity that exists through equity, debt, or other means and includes any indirect ownership or investment interest no matter how many levels removed from a direct interest.

A financial interest/relationship may arise from the following non-exclusive examples:

(a) Compensation, including wages, salaries, commissions, professional fees, or fees for business referrals;
(b) Current or known future arrangements or requirements for which you are defined as an interested party including, but not limited to, an entity that may create one or more of the three forms of COI;
(c) Consulting relationships, including commercial and professional consulting and service arrangements, scientific and technical advisory board memberships, or serving as an expert witness in litigation;
(d) Services provided in exchange for honorariums including travel expense reimbursements;

(e) Research funding or other forms of research support;
(f) Healthcare related investment in the form of stock or bond ownership, including healthcare sector investment only mutual funds;
(g) Healthcare business ownership or partnership interests;
(h) Patents, copyrights, and other intellectual property interests;
(i) Seeking or negotiating for prospective employment or business; or
(j) Gifts, including travel.

Mitigation – means action taken by the Contractor to reduce the COI risk to a level acceptable to CMS on a present contract.

Organizational Conflict of Interest – In accordance with FAR 2.101 Definitions, means that because of other activities or relationships with other persons, a person is unable, or potentially unable, to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is, or might be, otherwise impaired, or a person has an unfair competitive advantage.

For purposes of this contract, the COI definition includes direct or indirect relationships including, but not limited to, the Contractor and its parent company, subsidiaries, affiliates, subcontractors, clients and principals.

Personal Conflicts of Interest – A situation in which a person has a financial interest, personal activity, or relationship that could impair the person's ability to act impartially and in the best interest of the Government when performing under this contract.

(a) Among the sources of personal conflicts of interest are—
  i. Financial interests of the person, spouse/domestic partner and/or any other dependent of the person, as defined for Federal tax purposes;
  ii. Other employment or financial relationships (including seeking or negotiating for prospective employment or business) and,
  iii. Gifts, including travel.

(b) For example, financial interests referred to in paragraph (a)(i) of this definition may arise from—
  i. Compensation, including wages, salaries, commissions, professional fees, or fees for business referrals;
  ii. Consulting relationships;
  iii. Services provided in exchange for honoraria or travel expense reimbursements;
  iv. Research funding or other forms of research support;
  v. Healthcare related investments;
  vi. Real estate investments;
  vii. Patents, copyrights, and other intellectual property interests; or
  viii. Business ownership and investment interests.

Potential COI – means that the COI could become an actual COI due to contingency events and/or as determined by CMS. This form of COI will require mitigation acceptable to CMS.

Principal – As defined in FAR 52.203-13, Contractor Code of Business Ethics and Conduct, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager, plant manager, head of a division or business segment, and similar positions).

Three (3) Types of COIs include:

Conflict Types	Definitions
Biased Ground Rules	Consists of situations in which a firm, as part of its performance of a Government contract, has helped (or is in a position to help) set the ground rules for another Government contract by, for example, writing the statement of work or the specifications, or establishing source-selection criteria. In these "biased ground rules" cases, the primary concern is that the firm could skew the competition, whether intentionally or not, in favor of itself and/or its affiliates.
Impaired Objectivity	Consists of situations where a firm has an interest (typically financial) that may conflict with the interest of the Government to whom the firm has a contractual obligation, and the firm's work under the Government contract could give the firm the opportunity to benefit its other business interests. If the firm is providing recommendations, judgment or advice, and its other business interests could be affected by that recommendation, judgment or advice, the firm's objectivity may be impaired. An example is where the firm was evaluating itself, an affiliate or a competitor, either through an assessment of performance under another contract or an evaluation of proposals.
Unequal Access to Information	"Unfair" access to non-public information – Consists of situations in which a firm has access to nonpublic information (including proprietary information and non-public source-selection information) as part of its performance of a Government contract and that information may provide the firm with a competitive advantage in a later competition for a Government contract. In these "unequal access to information" cases, the concern is limited to the risk of the firm gaining an unfair competitive advantage; there is no issue of bias. Note: Incumbency alone does not constitute an "unequal access to information."

c. Conflicts of Interest Identified During Contract Performance – In accordance with FAR 3.10 and 52.203-13, Contractor Code of Business Ethics and Conduct, and

this contract, the Contractor shall have procedures in place to detect and disclose all COIs throughout the life of the contract.

1. **COI Oversight Program:** The Contractor shall maintain an effective COI Oversight Program. As part of the program, the Contractor shall implement company business practices, procedures, polices and internal controls for compliance with COI requirements, such as:

   (a) Preventing conflicts of interest, prohibiting the use of non-public information accessed through this contract for personal gain, and obtaining a signed non-disclosure agreement to prohibit disclosure of non-public information accessed through this contract;
   (b) Conducting Internal and External Audits;
   (c) Policy Enforcement and Employee Disciplinary Actions;
   (d) Retention of Records;
   (e) Management of Subcontractors;
   (f) Internal control systems;
   (g) Display of Fraud Hotline Poster(s) in accordance with FAR 52.203-14 Display of Hotline Poster(s).
   (h) Reviewing the information required by Attachment J.8, Contractor Personal Conflict of Interest Financial Disclosure Template, for each principal, officer and governing body member (e.g., Board of Directors; Trustees; etc.) of the organization, as well as managers and key personnel who would be, or are involved with, the performance of this contract. It is recommended that individuals who have not disclosed changes within the reporting period, submit an annual disclosure update to their Compliance Officer for review;
   (i) Informing employees, through an employee education and training program, of their obligation to disclose and prevent conflicts of interest, not to use non-public information accessed through performance of this contract for personal gain, and to avoid even the appearance of personal conflicts of interest; and,
   (j) Reporting to the Contracting Officer any conflict of interest violations.

The following details are provided for respective COI disclosure expectations when/if a COI arises during contract performance:

2. **Conflict of Interest:** COI information shall be submitted as follows:

(a) Conflict of Interest Submission During Contract Performance:

At any time during the performance of this contract, if the Contractor learns of any actual, potential, or apparent COI, whereby a reasonable business person might equate the COI to one (1) of the three (3) types of COIs identified in H.1.b Definitions, the Contractor shall notify the Contracting Officer in writing within five (5) business days of the identification of the actual, potential, or apparent COI. Within 30 calendar days, or as otherwise negotiated with the Contracting Officer, the Contractor shall submit a COI Disclosure in accordance with 2(b)

below.

(b) What is Required in a COI Disclosure: When an initial COI disclosure is submitted and/or a revision thereof is required, the Contractor shall provide an initial or revised, as the case may be, Attachment J.7, Contractor Business Ethics, Conflict of Interest and Compliance Program Requirements.

(c) Personal COI Information: It is the Offeror/Contractor's responsibility to have a plan in place (see H.1.c.1 COI Oversight Program) to ensure that actual, potential, or apparent personal conflicts of interest are identified, analyzed and mitigated for performance of this contract.

Personal COI information shall be obtained by the Offeror/Contractor for each:

- Manager or Key personnel who would be, or are involved with, the performance of this contract;
- Governing Body member (e.g., Board of Directors, Trustees, etc.); and,
- Principals of the organization as defined by FAR 52.203-13, Contractor Code of Business Ethics and Conduct.

Attachment J.8, Contractor Personal Conflict of Interest Financial Disclosure Template is provided as a "sample" for the Offeror/Contractor to follow when identifying, analyzing and mitigating actual, potential, or apparent Personal COIs for this contract. Notwithstanding, Personal COI information obtained from the above individuals shall not be submitted to the Government.

(d) Mitigation/Resolution: The Contracting Officer determines whether a COI has been identified and whether the actual, potential or apparent COI has been mitigated/resolved to the Government's satisfaction. The Mitigation/Resolution plan may include a COI audit requirement as determined by the Contracting Officer. The Contractor's approved COI Mitigation/Resolution plan shall be incorporated into the contract.

In cases whereby a COI cannot be, or has not been, mitigated to the Contracting Officer's satisfaction, the Contracting Officer may take the following action including, but not limited to:

i. Request a post-award waiver in accordance with FAR 9.503 Waiver, from the Head of the Contracting Activity; or
ii. Make changes to the requirements of the contract; or
iii. Terminate the contract.

(e) Independent Audit: If the Contracting Officer requires a COI audit as part of the accepted mitigation plan, the Contractor shall obtain the services of an External/Independent auditor to conduct an audit. If the Government chooses to undertake the audit in lieu of the Contractor's independent auditor, the Contracting Officer will notify the Contractor within 60 days of the anniversary

date of the contract.

Such auditor shall have expertise in conducting compliance program and conflict of interest audits. The Contractor's records may also be subject to audit by the Government to ensure compliance with this contract's H.1 clause requirements and/or ensure that any corrective action, if necessary, has been implemented.

1. Subcontractors: A COI independent audit shall be required at the discretion of the Prime Contractor. If the Prime Contractor requires an audit of the subcontractor(s), the subcontractor's audit shall be included with the Prime Contractor's audit submission.

2. First Audit: When an audit is required as part of an acceptable mitigation plan, the Contracting Officer will negotiate the frequency of the audits and required deliverable dates. Generally, only one audit will be required during the period of performance subject to Contracting Officer discretion. The independent audit will be submitted by the auditor directly to the Contracting Officer with a copy to the Contractor.

3. Subsequent Audits: Additional audits are at the discretion of the Contracting Officer. The Contracting Officer will consider previous audit findings, any corrective action(s) and any new COI information, when making the decision to require subsequent audits.

4. Audit Findings: When Contractor Conflict of Interest Oversight findings are disclosed in an independent audit, the Contractor shall include in the draft audit report its proposed corrective action plan for each finding. The Contracting Officer may require a revised COI mitigation plan to be submitted as a result of the audit findings.

5. Independent Audit Requirements:

   (a) The auditor shall decide what processes it will use to review, verify and confirm the information, processes and policies disclosed by the Contractor to the Government. The audit shall include a process for the contractor to review audit findings and provide a response to the auditor, which shall be included in the final audit submitted to the CMS Contracting Officer.

   (b) The audit shall confirm that any and all COI mitigation plans, approved by the Government, have been implemented and are functioning as anticipated. Although not all inclusive, the auditor may also want to consider the following:

      (i) Review of all COI disclosures submitted to the Government to validate the accuracy and completeness of such disclosures;

(ii) Conducting appropriate interviews with principals, key personnel and independent members of the board of directors, as appropriate;
(iii) Reviewing the Contractor's organizational chart(s), articles of incorporation, bylaws and/or other documents, to validate the accuracy and completeness of COI disclosures to the Government;
(iv) Confirming that the Contractor annually, at a minimum, collects and reviews for assessment and appropriate action by the Compliance Officer, personal conflict information from its principals, key personnel (on the relevant contract(s)) and board of director members;
(v) Confirming whether the Contractor is in compliance with its internal Contractor Conflict of Interest Oversight program(s); and,
(vi) For its Subcontractors, confirming whether the prime Contractor is monitoring Subcontractor compliance with the required contract flow-down provisions and disclosed practices, in accordance with contract H.1. The auditor may review other information as it deems appropriate to ensure that COI issues have been identified and resolved, in accordance with Contractor disclosures.
(vii) The auditor will also examine the Contractor's records to verify that all of the requirements specified in FAR 52.203-13(c)(2)(ii), Contractor Code of Business Ethics and Conduct, are met.

6. Reporting Requirements: The audit report, inclusive of all auditor findings and proposed corrective actions, shall be delivered via e-mail or US Postal Service to the Contracting Officer directly from the auditor.

d. Subsequent COI Disclosures (i) When/if a COI is discovered during contract performance, subsequent COI disclosures may be required as follows:

- If as a result of, the Government or Contractor independent auditor review, any findings require a change in the Initial Disclosure, submit a COI Disclosure Revision, in accordance d (ii). below, to the Contracting Officer within 30 calendar days of the final audit report.
- Within 30 calendar days when the Contracting Officer requests a revision.
- At least 45 calendar days prior to a change due to proposed or planned business actions, e.g., acquiring or selling a business or business segment, changes in ownership of the organization holding the contract, etc.

(ii)What is Required in a Revision:

When COI disclosures require revision, the Contractor shall provide a revised

Attachment J.7, Contractor Business Ethics, Conflict of Interest and Compliance Program Requirements. Red-lined versions are preferred.

e. Subcontractor Flow-Down Clause: The prime Contractor is responsible for avoiding, neutralizing and mitigating all actual, potential, or apparent COIs of its Subcontractors, in accordance with this clause. Therefore, the prime Contractor shall flow-down H.1 Post Award Business Ethics, Conflict of Interest and Compliance, of this contract in all subcontracts. For Subcontractors, wherever the term "Contractor" is used, insert "Subcontractor."

H.4 CMS INFORMATION SECURITY (APR 2013)

All CMS information shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional, in order to maintain the security, confidentiality, integrity, and availability of such information. Therefore, if this contract requires the contractor to provide services (both commercial and non-commercial) for Federal Information/Data, to include any of the following requirements:

- Process any Information/Data; or
- Store any Information/Data (includes "Cloud" computing services); or
- Facilitate the transport of Information/Data; or
- Host/maintain Information/Data (including software and/or infrastructure developer/maintainers); or
- Have access to, or use of, Personally Identifiable Information (PII), including instances of remote access to, or physical removal of, such information beyond agency premises or control,

The contractor shall become and remain compliant with the requirements set forth at the CMS Information Security website at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Security-Contract-Clause-Provision.html. The requirements cover **all** CMS contracts and associated deliverables, which are required on a "per contractor" basis.

The contractor shall ensure that the following Federal information security standards are met for all of its CMS contracts:

- **Federal Information Security Management Act (FISMA)** – FISMA information can be found at http://csrc.nist.gov/groups/SMA/fisma/index.html. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source; and,
- **Federal Risk and Authorization Management Program (FedRAMP)** – FedRAMP information can be found at http://www.gsa.gov/portal/category/102371. The FedRAMP is a government-

wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The Contractor shall include in all awarded subcontracts the FISMA/FedRAMP compliance requirements set forth at the CMS Information Security website at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Security-Contract-Clause-Provision.html..

H.5 HIPAA BUSINESS ASSOCIATE CLAUSE (OCT 2014)

All Protected Health Information (PHI), as defined in 45 C.F.R. §160.103, that is relevant to this Contract, shall be administered in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA," 42 U.S.C. § 1320d), as amended, as well as the corresponding implementing regulations and this HIPAA Business Associate Clause.

a. Definitions:
All terms used herein and not otherwise defined, shall have the same meaning as in HIPAA, as amended, and the corresponding implementing regulations. Non-HIPAA related provisions governing the Contractor's duties and obligations, such as those under the Privacy Act and any applicable data use agreements, are generally covered elsewhere in the Contract.

The following definitions apply to this Contract Clause:

"**Business Associate**" shall mean the Contractor (and/or the Contractor's subcontractors or agents) if/when it uses individually identifiable health information on behalf of CMS, i.e. PHI, to carry out CMS' HIPAA-covered functions.

"**Covered Entity**" shall mean the portions of CMS that are subject to the HIPAA Privacy Rule.

"**Secretary**" shall mean the Secretary of the Department of Health & Human Services or the Secretary's designee.

b. Obligations and Activities of Business Associate:
Except as otherwise provided in this Contract, Business Associate, as defined above, shall only use or disclose PHI on behalf of, or to provide services to, Covered Entity in accordance with this Contract and the HIPAA Privacy and Security Rules.

Business Associate shall document in writing the policies and procedures that will be used to meet HIPAA requirements. The policies and procedures shall include the following, at a minimum:

1. Business Associate shall not:
    i. Use or disclose PHI that is created, received, maintained or transmitted

by Business Associate from, or on behalf of, Covered Entity other than as permitted or required by this Contract or as required by law;

ii. Sell PHI; or,

iii. Threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual for:

A. Filing a complaint under 45 CFR § 160.306;

B. Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under 45 CFR Part 160; or

C. Opposing any act or practice that is unlawful under HIPAA, provided there is a good faith belief that the practice is unlawful, the manner of opposition is reasonable, and the opposition does not involve the disclosure of PHI in violation of subpart E of Part 164.

2. Business Associate shall:

i. Have a security official who will be responsible for development and implementation of its security policies and procedures, including workforce security measures, to ensure proper security awareness and training (including security incident response and reporting), and security incident procedures, in accordance with this Contract, including this HIPAA Business Associate Clause and the Contract's clause entitled "CMS Information Security."

ii. Use administrative, physical and technical safeguards to prevent use or disclosure of PHI created, received, maintained or transmitted by Business Associate from, or on behalf of Covered Entity only as provided for by this Contract. In doing so, it shall implement policies and procedures to address the following and, where applicable, ensure that such policies and procedures are also in conformance with this Contract's clause entitled "CMS Information Security:"

A. Prevent, detect, contain and correct security violations through the use of:

a. Risk analyses (including periodic technical and nontechnical evaluations);

b. Appropriate risk management strategies, including system activity review;

c. Information access procedures for approving individual's access rights to PHI (including the implementation of workforce security measures to ensure continued appropriate role-based access to PHI), and technical policies and procedures to ensure compliance with grants of access (including unique user identification and tracking of users) and;

d. The imposition of sanctions for violations.

B. Limit physical access to its electronic information systems and the

facility or facilities in which they are housed.

C. Implement policies, procedures and physical security measures that will limit access to PHI through workstations and other devices, including access through mobile devices.
D. Implement media controls covering the movement of devices containing PHI within or outside of the Business Associate's facility as well as the disposal and reuse of media containing PHI.
E. Implement appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability (including the use of contingency plans) of any electronic protected health information ("EPHI") it creates, receives, maintains or transmits from, or on behalf of the Covered Entity to prevent impermissible use, disclosure, maintenance or transmission of such EPHI. In the establishment of such safeguards, Business Associate shall consider its size, complexity and capabilities, as well as its technical infrastructure, and its hardware and software security capabilities.

iii. Assess, and implement, where appropriate, any addressable implementation specifications associated with applicable PHI security standards.
iv. Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Contract.
v. Comply with the following Incident Reporting:

A. Report to Covered Entity any security incident/breach involving unsecured PHI, of which it becomes aware, including those of its agents and subcontractors. The Business Associate shall report any violation of the terms of this contract involving PHI and any security incidents/breaches involving unsecured PHI to CMS within one (1) hour of discovery in accordance with the CMS Risk Management Handbook (RMH), specifically "RMH Vol II Procedure 7-2 Incident Handling Procedure" and "RMH Vol III Standard 7-1 Incident Handling." These procedures can be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html In addition, the Business Associate will also notify the CMS Contracting Officer and the Contracting Officer's Representative (COR) by email within one (1) hour of identifying such violation or incident.
B. Upon Covered Entity's knowledge of any material security incident/breach by Business Associate, Covered Entity will provide an opportunity for Business Associate to cure the breach or

end the violation consistent with the termination clause of this Contract. *See also* paragraph D. Term of Clause below.

vi. Ensure that any agent or subcontractor agrees through a written contract, or other legally enforceable arrangement, to the same restrictions and conditions that apply through this HIPAA Contract Clause, when creating, receiving, maintaining or transmitting PHI from, or on behalf of, Covered Entity.

vii. Upon Covered Entity's request:
   A. Provide the Covered Entity or its designee with access to the PHI created, received, maintained or transmitted by Business Associate from or on behalf of the Covered Entity in the course of contract performance in order to ensure Covered Entity's ability to meet the requirements under 45 CFR § 164.524.
   B. Amend PHI as Covered Entity directs or agrees to pursuant to 45 CFR § 164.526.

viii. Make its facilities and any books, records, accounts, and any sources of PHI, including any policies and procedures, that are pertinent to ascertaining its own compliance with this contract or the Covered Entity's compliance with the applicable HIPAA requirements, available to Covered Entity, or, in the context of an investigation or compliance review, to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the various rules implementing the HIPAA.

ix. Document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

x. Provide to Covered Entity, or an individual identified by the Covered Entity, information collected under this Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

xi. Make reasonable efforts to limit the PHI it uses, discloses or requests to the minimum necessary to accomplish the intended purpose of the permitted use, disclosure or request.

c. Obligations of Covered Entity

Covered Entity shall notify Business Associate of any:

1. Limitation(s) in its Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI;

2. Changes in, or revocation of, permission by an Individual to use or disclose

their PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI; and,

3. Restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d. Term of Clause

1. The term of this Clause shall be effective as of date of Contract award, and shall terminate when all of the PHI provided to Business Associate by the Covered Entity or a Business Associate of the Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity in accordance with "CMS Information Security" procedures. Business Associate shall not retain any PHI.

2. Security Incident/Breach:

   Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall take action consistent with the terms of this Contract, and, as appropriate, the following:

   i. Federal Acquisition Regulation (FAR) Contracts – Covered Entity may:
      A. Terminate this Contract in accordance with FAR Part 49, Termination of Contracts, if the Business Associate does not cure the security incident/breach within the time specified by Covered Entity and/or cure is not possible; or,
      B. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

   ii. Other Agreements –Covered Entity shall either:
      A. Provide an opportunity for Business Associate to cure the breach or end the violation consistent with the termination terms of this Contract. Covered Entity may terminate this Contract for default if the Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or,
      B. Consistent with the terms of this Contract, terminate this Contract for default if Business Associate has breached a material term of this Contract and cure is not possible; or,
      C. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

3. Returning or Destroying PHI:

   Business Associate, as defined above, which includes subcontractors or agents of the Contractor, shall:

i. Upon expiration or termination of this Contract, for any reason, return or destroy all PHI received from Covered Entity or another Business Associate of the Covered Entity, as well as any PHI created, received, maintained or transmitted from or on behalf of Covered Entity, or another Business Associate of the Covered Entity, in accordance with this contract, including the "CMS Information Security" clause.

ii. In the event that Business Associate determines that returning or destroying the PHI is infeasible, provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon such notice that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

e. Miscellaneous

1. A reference in this Contract to a section in the Rules issued under HIPAA means the section as in effect or as amended.
2. The respective rights and obligations of Business Associate under paragraph D.3.b of the section entitled "Term of Clause" shall survive the termination of this Contract.

Any ambiguity in this Contract clause shall be resolved to permit Covered Entity to comply with the Rules implemented under HIPAA.

H.6 OPEN GOVERNMENT PROACTIVE PREDISCLOSURE NOTIFICATION (OCT 2013)

In order to reduce the administrative burden of responding to Freedom of Information Act (FOIA) requests for high visibility/high public interest contracts throughout contract administration, the Contractor shall submit its review of the awarded contract (and contract modifications, if requested) for FOIA disclosure exemptions within thirty (30) calendar days of contract award. The review will substantiate "…Trade secrets and commercial or financial information obtained from a person and privileged or confidential…" information, in accordance with 5 U.S.C. §552 FOIA, Exemption (b)(4), which could reasonably be expected to cause substantial competitive harm.

Submissions: The Contractor shall submit one (1) Compact Disc (CD) or Digital Video Disc (DVD) with all 5 U.S.C. §552 FOIA, Exemption (b)(4), "…Trade Secrets, Commercial or Financial Information Which is Privileged or Confidential…," otherwise known as public release/non-Confidential Business Information (non-CBI), with the information identified as follows:

a. CBI Highlighted Copy of Contract: One copy of the contract with all CBI highlighted for CMS FOIA review.

b. Contractor Proposed Redacted Public Release Copy of Contract: An additional copy of the contract will be provided for public release with all the identified information redacted. Redactions shall be made using "black" boxes, which cannot be removed or uncovered by a reader.

c. Pre-Disclosure Concerns - Comments/Rationale for Non-Disclosure of Trade Secrets, Commercial or Financial Information Which is Privileged or Confidential: The Contractor shall provide, in a separate file, rationale for why disclosure of "…Trade Secrets, Commercial or Financial Information Which is Privileged or Confidential…" would cause the Contractor organization substantial competitive harm if disclosed to other entities. Rationale shall be provided for each individual recommended redaction. Generalized conclusions of competitive harm are not a sufficient basis for the CMS FOIA office to invoke the exemption and thereby protect the Contractor's interest.

All CD/DVDs shall be mailed to the CMS FOIA Officer (address below) within thirty (30) calendar days of contract award and within thirty (30) calendar days of a CMS request, i.e. existing or modified contracts. All CD/DVD files shall be submitted as Portable Document Format (.pdf) files.

CD/DVD and File Naming Conventions: The Contractor shall name the CD/DVD with the Contract Number and utilize the following CD/DVD file naming conventions:

HHSM-500-2013-xxxxxx – Highlighted
HHSM-500-2013-xxxxxx – Redacted
HHSM-500-2013-xxxxxx – Pre-Disclosure Concerns

CD/DVD shall be mailed to the CMS FOIA Officer at:

Centers for Medicare & Medicaid Services
Freedom of Information Act Office
ATTN: CMS FOIA Officer
Mailstop: N2-20-16
7500 Security Boulevard
Baltimore, MD 21244-1850

Copy– Correspondence Only (No CD/DVD):

- Contracting Officer
- Contracting Officer's Representative (COR)

It should be noted that the CMS FOIA Office makes the final determination as to what information is released to the public, after considering any feedback from OAGM and/or the Contractor.

H.7 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 reg-ular place of business. If the employee's work involves recur-ring 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 https://nbib.opm.gov/hr-security-personnel/investigations-billing-rates-resources/. 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.

H.8 RESTRICTIONS AGAINST DISCLOSURE

(a) The Contractor agrees to keep all information it gathers or analyzes or information the Government in the course of this contract/task order/delivery order furnishes in the

strictest confidence. The Contractor also agrees that Government-provided information marked "For Official Use Only," "Confidential", or "Proprietary" must also be similarly protected and shall take all reasonable measures necessary to prohibit access to such information by any such person other than those Contractor employees needing such information to perform the work, i.e., on a need-to-know basis.

(b) The Contractor shall immediately notify the Contracting Officer in writing in the event it has been determined or the Contractor has reason to suspect a breach of this requirement.

(c) The Contractor shall require that all employees and consultants who are given access to such information sign a confidentiality and nondisclosure statement agreeing to safeguard the confidentiality of all such information gathered or provided to them hereunder as an integral condition of their employment.

(d) Upon the Government's written request, the Contractor shall provide the Contracting Officer with plans and procedures to ensure the confidentiality and physical security of information gathered or provided hereunder.

(e) The Contractor may "gather and analyze" information that is not furnished or owned by the Government. Such information shall not be subject to the restrictions in this clause.

H.9 CONTRACTOR TERMINATION CMS BUILDING PASS

In the event that the contractor terminates an employee working on this contract, or an employee working on this contract voluntarily leaves the employment of the contractor and that employee has been issued a contractor's badge by CMS for access to CMS Buildings; The contractor shall immediately take the following actions:

- Secure the CMS contractor's badge from the employee;
- Formally advise the contracting officer that the individual is no longer an employee of the contractor, and;

- Return the badge with the notification to the contracting officer.

H.10 SECURITY CLAUSE-BACKGROUND-INVESTIGATIONS FOR CONTRACTOR PERSONNEL

A. If applicable, Contractor personnel performing services for CMS under this contract, task order or delivery order shall be required to undergo a background investigation. CMS will pay for the background investigations.

B. After contract award, the CMS COR and the Emergency Management & Response Group (EMRG), with the assistance of the Contractor, shall perform a

position-sensitivity analysis based on the duties contractor personnel shall perform on the contract, task order or delivery order. The results of the position-sensitivity analysis will determine first, whether the provisions of this clause are applicable to the contract and second, if applicable, determine each position's sensitivity level (i.e., high risk, moderate risk or low risk) and dictate the appropriate level of background investigation to be processed. Investigative packages may contain the following forms:

1. SF-85, Questionnaire for Non-Sensitive Positions, 09/1995
2. SF-85P, Questionnaire for Public Trust Positions, 09/1995
3. OF-612, Optional Application for Federal Employment, 12/2002
4. OF-306, Declaration for Federal Employment, 01/2001
5. Credit Report Release Form
6. FD-258, Fingerprint Card, 5/99, and
7. CMS-730A, Request for Physical Access to CMS Facilities (NON-CMS ONLY), 11/2003.

C. The Contractor personnel shall be required to undergo a background investigation commensurate with one of these position-sensitivity levels:

(i) High Risk (Level 6)

Public Trust positions that would have a potential for exceptionally serious impact on the integrity and efficiency of the service. This would include computer security of a major automated information system (AIS). This includes positions in which the incumbent's actions or inaction could diminish public confidence in the integrity, efficiency, or effectiveness of assigned government activities, whether or not actual damage occurs, particularly if duties are especially critical to the agency or program mission with a broad scope of responsibility and authority.

Major responsibilities that would require this level include:

a. development and administration of CMS computer security programs, including direction and control of risk analysis and/or threat assessment;
b. significant involvement in mission-critical systems;
c. preparation or approval of data for input into a system which does not necessarily involve personal access to the system but with relatively high risk of causing grave damage or realizing significant personal gain;
d. other responsibilities that involve relatively high risk of causing damage or realizing personal gain;
e. policy implementation;
f. higher level management duties/assignments or major program responsibility; or
g. independent spokespersons or non-management position with authority for independent action.

Approximate cost of each investigation: $3,500

(ii) Moderate Risk (Level 5)

Public Trust positions that have potential for moderate to serious impact on the integrity and efficiency of the service, including computer security. These positions involve duties of considerable importance to the CMS mission with significant program responsibilities that could cause damage to large portions of AIS. Duties involved are considerably important to the agency or program mission with significant program responsibility, or delivery of service. Responsibilities that would require this level include:

a. the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the system;
b. systems design, operation, testing, maintenance, and/or monitoring that are carried out under the technical review of a higher authority at the High Risk level;
c. access to and/or processing of information requiring protection under the Privacy Act of 1974;
d. assists in policy development and implementation;
e. mid-level management duties/assignments;
f. any position with responsibility for independent or semi-independent action; or
g. delivery of service positions that demand public confidence or trust.

Approximate cost range of each investigation: $150 - $2,600

(iii) Low Risk (Level 1)

Positions having the potential for limited interaction with the agency or program mission, so the potential for impact on the integrity and efficiency of the service is small. This includes computer security impact on AIS.

Approximate cost of each investigation: $100

D. The Contractor shall submit the investigative package(s) to the EMRG within three (3) days after being advised by the EMRG of the need to submit packages. Investigative packages shall be submitted to the following address:

Centers for Medicare & Medicaid Services
Office of Operations Management
Emergency Management & Response Group
Mail Stop SL-13-15
7500 Security Boulevard
Baltimore, Maryland 21244-1850

E. The Contractor shall submit a copy of the transmittal letter to the Contracting Officer (CO).

F. Contractor personnel shall submit a CMS-730A (Request for Badge) to the EMRG. The Contractor and the COR shall obtain all necessary signatures on the CMS-730A prior to any Contractor employee arriving for fingerprinting and badge processing.

G. The Contractor must appoint a Security Investigation Liaison as a point of contact to resolve any issues of inaccurate or incomplete form(s). Where personal information is involved, EMRG may need to contact the contractor employee directly. The Security Investigation Liaison may be required to facilitate such contact.

H. After EMRG fingerprints contractor personnel and issues them a temporary CMS identification badge, the EMRG will send their completed investigative package to the Office of Personnel Management (OPM). OPM will conduct the background investigation. Badges will be provided by EMRG while contractor personnel investigative forms are being processed. The Contractor remains fully responsible for ensuring contract, task order or delivery order performance pending completion of background investigations of contractor personnel.

I. EMRG shall provide written notification to the CO with a copy to the COR of all suitability decisions. The shall then notify the Contractor in writing of the approval of the Contractor's employee(s), at that time the Contractor's employee(s) will receive a permanent identification badge. Contractor personnel who the EMRG determines to be ineligible may be required to cease working on the contract immediately.

J. The Contractor shall report immediately in writing to EMRG with copies to the CO and the COR, any adverse information regarding any of its employees that may impact their ability to perform under this contract, task order or delivery order. Reports should be based on reliable and substantiated information, not on rumor or innuendo. The report shall include the contractor employee's name and social security number, along with the adverse information being reported.

K. Contractor personnel shall be provided an opportunity to explain or refute unfavorable information found in an investigation to EMRG before an adverse adjudication is made. Contractor personnel may request, in writing, a copy of their own investigative results by contacting:

Office of Personnel Management
Freedom of Information
Federal Investigations Processing Center
PO Box 618
Boyers, PA 16018-0618.

L. 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, task order, or delivery order within one (1) year from the date the background investigation was completed, then the Contractor may be required to reimburse CMS for the full cost of the investigation. Depending upon the type of background investigation conducted, the cost could be approximately $100 to $3,500. 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

M. The Contractor must immediately provide written notification to EMRG (with copies to the CO and the COR) of all terminations or resignations of Contractor personnel working on this contract, task order or delivery order. The Contractor must also notify EMRG (with copies to the CO and the COR) when a Contractor's employee is no longer working on this contract, task order or delivery order.

N. At the conclusion of the contract, task order or delivery order and at the time when a contractor employee is no longer working on the contract, task order or delivery order due to termination or resignation, all CMS-issued parking permits, identification badges, access cards, and/or keys must be promptly returned to EMRG. Contractor personnel who do not return their government-issued parking permits, identification badges, access cards, and/or keys within 48 hours of the last day of authorized access shall be permanently barred from the CMS complex and subject to fines and penalties authorized by applicable federal and State laws.

H.11 ADP SYSTEMS SECURITY REQUIREMENTS

In the performance of this contract, the Contractor agrees to comply with the ADP systems security requirements of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", and with the ADP systems security policy of DHHS as outlined in Part 6 of the HHS ADP Systems Manual and in CMS's AIS Guide. The Contractor shall include this requirement in any subcontract awarded under this prime contract

H.12 352.211.3 PAPERWORK REDUCTION ACT (DEC 2015)

In the event that it becomes a requirement to collect information under this order, OMB

Forms clearance shall be required pursuant to the Paperwork Reduction Act (see 5 CTR, Part 1320). The Contractor is hereby advised not to expend any funds or take any other action to solicit information until the Contracting Officer has notified the Contractor in writing that the required OMB clearance has been obtained. The Contractor shall provide to the COR such information as will facilitate obtaining such clearance.

H.13 HHSAR 352.224-70 PRIVACY ACT (DEC 2015)

This contract requires the Contractor to perform one or more of the following: (a) design; (b) develop; or (c) operate a federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) [**5 U.S.C. 552a(m)(1)**] and applicable agency regulations. The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties [**5 U.S.C. 552a(i)**]. The Contractor shall ensure that each of its employees knows the prescribed rules of conduct and that each employee is aware that he/she is subject to criminal penalties for violation of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under this contract which require the design, development or operation of the designated system(s) of records [**5 U.S.C. 552a(m)(1)**]. The contract work statement: (a) identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and (b) specifies the disposition to be made of such records upon completion of contract performance.