Appendix A: CMS Clauses

G.1. PAYMENTS - INVOICES – (August 2020)

1. GENERAL: Effective August 31, 2020, the contractor/vendor shall create an invoice within the Invoice Processing Platform (IPP), a secure Web-based service for federal agencies and their vendors to manage government invoicing from purchase order (PO) through payment notification. Note: All invoice terms and conditions are contract specific and may vary from contract to contract.

2. CONTENT OF INVOICE: FAR 32.905 Payment Documentation and Process, provides the required content for a proper invoice. In addition to the requirements of FAR 32.905, the following items shall also be included on the invoice to be considered proper:

- Line item number (i.e. CLIN/SLIN as applicable);
- Contractor's DUNS Number;
- Period of performance or delivery date of goods or services provided;
- Attachments

3. INVOICE SUBMISSION: The contractor/vendor shall create an invoice from the Purchase Order (PO)/Contract via the IPP website http://www.ipp.gov/. For questions, call IPP Customer Support at (866) 973-3131 or email the IPP Customer Support at IPPCustomerSupport@fiscal.treasury.gov.

4. PAYMENTS: The Government shall make payment of all proper invoices in accordance with the following clauses:

- FAR 52.232-33 Payments by Electronic Funds Transfer – System for Award Management,
- FAR 52.232-1 Payments
- FAR 52.212-4 Contract Terms and Conditions – Commercial Items (If applicable)
- FAR 52.216-7 Allowable Cost and Payment
- FAR 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts

Payment shall be made upon acceptance by the Contracting Officer's Representative (COR)in accordance with the applicable FAR Inspection and Acceptance clause and the Contracting Officer's approval, as appropriate.

Reimbursement for invoices submitted under this contract shall be made no later than 30 calendar days after receipt of a proper invoice from the Contractor requested at the paying office designated above. Contracts with a 15-day payment term are not subject to interest payments until after day 30.

5. INTEREST ON OVERDUE PAYMENT: The Prompt Payment Act, Public Law 97-177 (96 Stat.85.31 U.S.C. 1801) is applicable to payments under this contract and requires the payment of interest on payments made more than 30 calendar days after receipt of a proper invoice in IPP.

Determinations of interest due will be made in accordance with the provisions of the Prompt Payment Act and 5 CFR 1315.

(end of clause)

G.2 CONTRACTOR PAST PERFORMANCE EVALUATION(S) (OCT 2014)

a. General:

In accordance with Federal Acquisition Regulation (FAR) 42.15, Contractor Performance Information, past performance evaluations shall be prepared at least annually and at the time the work under a contract or order is completed. Additional interim performance evaluations may be prepared at Contracting Officer discretion, as necessary.

CMS will utilize the Contractor Performance Assessment Reporting System (CPARS), the Government-wide evaluation reporting tool for all past performance reports on contracts and orders, as appropriate. CPARS is a secure Internet website located at https://www.cpars.gov.

b. CPARS Process:

1. CPARS Training: Contractors may obtain CPARS training material and register for on-line training https://www.cpars.gov.
2. Post-Award Contract Registration: CMS is responsible for registering the contract in CPARS within 30 calendar days of contract award. The Contractor shall:
    1. Designate at least one (1) point of contact that will be responsible for serving as the Contractor's Representative (CR). Additional CRs may also be identified; and,
    2. Provide the CMS Contract Specialist with the name(s) and email address(es) of the CPARS point(s) of contact.

Once CMS registers the contract in CPARS, the CR(s) will receive an automated CPARS email message that contains User IDs and instructions for creating a password for future past performance evaluation processing.

3. Interim, Annual and Final Past Performance Evaluation Reports:

a. Issuing the Evaluation: Once the CMS Assessing Official (AO) issues an evaluation to the Contractor in CPARS, the CR(s) will receive an email instructing them to login to CPARS to review the evaluation.

b. Contractor Comments: The CR has the option to provide comments on the evaluation, indicate if they concur or do not concur with the evaluation, sign, and then return the evaluation

to the AO. The CR has a total of 60 days following the AO's evaluation signature date to submit comments. If the CR submits comments within the first 14 days following the AO's signature date and the AO closes the evaluation, the evaluation will become available in CPARS within 1 day. On day 15 following the AO's evaluation signature date, the evaluation will become available in CPARS with or without CR comments and whether or not it has been closed by the AO. If no CR comments have been sent and the evaluation has not been closed, it will be marked as "Pending" in CPARS. If the CR sends comments at any time prior to 61 days following the AO's evaluation signature date, those comments will be reflected in CPARS within 1 day. On day 61 following the AO's evaluation signature date, the CR will be "locked out" of the evaluation and may no longer send comments.

(end of clause)

G.3. Contractor Work Performed Outside the United States and its Territories (January 2021)

To comply with requirements of Homeland Security Presidential Directive -12 (HSPD-12) and Personal Identity Verification (PIV) of Federal Employees and Contractors, CMS must achieve appropriate security assurance for multiple CMS information systems by efficiently verifying the claimed identity of individuals working on the contract. The Contractor and its subcontractor(s) shall not perform any activities under this contract, including the transmission of data or other information, outside of the United States (U.S.) and its Territories without the prior written approval of the Contracting Officer. If work must be performed outside the U.S., the Contractor shall submit a request to the Contracting Officer, in writing, at least 45 calendar days prior to the work beginning.

The Contracting Officer will consider the following factors in making a decision whether to authorize the performance of work outside the U.S. and its Territories:

1. The necessity of the work to be performed outside the United States and its territories;
2. The Statement of Work under contract that will be performed outside the U.S. and its Territories;
3. Total projected dollar value of the work to be performed outside the U.S.;
4. Total projected number of labor hours and length of time to be performed for each individual employee working outside the U.S.;
5. The desired country/location where the work will be performed;
6. FAR Part 25, Foreign Acquisitions, and all other laws and regulations applicable to the performance of work outside the U.S.;
7. The contractor and/or its subcontractor(s) plans to adequately protect and secure CMS data, as well as abide by all applicable laws and regulations when work is performed outside of the U.S. and its Territories. Plans shall include -
    1. Adequate contract terms regarding system security;
    2. Adequate contract terms regarding the confidentiality and privacy requirements for information and data protection;
    3. Adequate contract terms that are otherwise relevant, including the requirements of the Statement of Work;

4. The Contractor's corporate compliance plan and internal policies and procedures designed to prevent and detect violations of applicable law, regulations, rules and ethical standards by employees, agents and others; and,

8. The necessity of Government Furnished Equipment (GFE) or Contractor Owned/Contractor Operated (COCO) devices to be used outside the U.S. and verification of a secure VPN access.
9. Compliance with Executive Order 13940 Aligning Federal Contracting and Hiring Practices With the Interests of American Workers. Determine if approval will reduce opportunities for the United States contractor workers performing in the United States and if this would cause any potential effects to national security.
10. Conformance with Section 889 "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment", of Public Law 115-232.
11. Determination that approval is in best interest of the Government.

The Contractor's request for authorization to perform work outside the U.S. shall include supplemental information to demonstrate that the performance of the work outside the U.S. satisfies all of the above factors. Contracting Officer approval to perform work outside the U.S. may require additional Statement of Work requirements, additional contract terms and conditions and/or Federal Acquisition Regulation (FAR) clauses to be incorporated into the contract.

(end of clause)

G.4 GOVERNMENT REPRESENTATIVES AND RESPONSIBILITIES (SEPT 2021)

Set forth below are the Government Representatives and their respective roles and responsibilities on this contract:

Contracting Officer: As defined in Federal Acquisition Regulation (FAR) 2.101, Definitions, and in accordance with FAR 1.602-1, Authority, "Contracting officers have authority to enter into, administer, and/or terminate contracts and make related determinations and findings." There is no other authorized representative or any other Administrative Contracting Officer assigned to this contract to carry out a Contracting Officer's duties, except for technical direction assigned to the Contracting Officer's Representative, if applicable.

The Contracting Officer is:

Centers for Medicare & Medicaid Services
Office of Acquisition & Grants Management
Information Technology Contracts Group
ATTN: Evelyn R. Dixon
7500 Security Blvd.
Mail-stop: B3-30-03
Baltimore, MD 21244-1850
Phone: 410-786-XXX
Email Address: Evelyn.Dixon1@cms.hhs.gov

Contract Specialist: Notwithstanding any of the other provisions of this Contract, the Contract Specialist will assist the Contracting Officer with his/her responsibilities as defined in the FAR.

Centers for Medicare & Medicaid Services
Office of Acquisition & Grants Management
Information Technology Contracts Group
ATTN: Erin Sparwasser
7500 Security Blvd.
Mail-stop: B3-30-03
Baltimore, MD 21244-1850
Phone: 410-786-xxxx
Email Address: Erin.Sparwasser@cms.hhs.gov

Contracting Officer's Representative: The Contracting Officer's Representative (COR), as defined in FAR 2.101, Definitions, is:

Centers for Medicare & Medicaid Services
Center for Medicare
ATTN: XXXX
7500 Security Blvd.
Baltimore, MD 21244-1850
Phone: 410-786-xxx
Email Address: xxxxxx@cms.hhs.gov

In accordance with FAR 1.602-2(d), Responsibilities, the COR's

In accordance with FAR 1.602-2(d), Responsibilities, the COR's delegated responsibilities are identified in the Contracting Officer's appointment memorandum, a copy of which will be furnished to the contractor.

The COR will serve as the primary liaison between the Contractor and the Contracting Officer and perform duties within the limitations of the COR's responsibilities in accordance with FAR 1.602-2(d).

Technical direction must be within the general scope of the work stated in the contract. The term "technical direction" is defined to include, without limitation, the following:

(1) Directions to the Contractor which direct the contract effort, shift work emphasis between work areas or tasks, require pursuit of certain lines of inquiry, fill in details or otherwise serve to accomplish the contractual technical requirements as identified in the Statement of Work or Performance Work Statement; or

(2) Provision of information to the Contractor, which assists in the interpretation of drawings, specifications, or technical portions of the work description.

Technical direction within the scope of the contract, shall be "in writing" whenever possible and routed through the CO prior to release to the Contractor. If technical direction is verbally communicated, the COR must immediately confirm its direction in writing. Where doubt exists as to whether proposed technical direction is within or outside the scope of the contract, the CO shall be contacted.

If, in the opinion of the Contractor, any instruction or direction issued by a Government representative constitutes a change to the contract or constitutes a "Change Order" as defined in FAR 2.101, Definitions, the Contractor shall follow the instructions identified in FAR 52.243-7 Notification of Changes.

The COR "has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract nor in any way direct the contractor or its subcontractors to operate in conflict with the contract terms and conditions" See FAR 1.202-2(d)(5). The COR's authority is not re-delegable and the COR may be personally liable for unauthorized acts in accordance with FAR 1.202-(d)(7)(iv) and (v). For example, the COR does not have the authority to: Make changes to contract terms and conditions; Direct the contractor to perform work or make deliveries not specifically required under the contract; Waive or relax the Government's rights with regard to the Contractor's compliance with the specifications, price, delivery or any other terms or conditions of the contract; Make any commitments or approve any actions that would create any financial obligation on the part of the Government; or Issue direction that constitutes a "change" as defined in: FAR 52.243-1, Changes – Fixed Price; FAR 52.243-2, Changes – Cost Reimbursement; FAR 52.243-3, Changes – Time and Material and Labor Hour; FAR 52.243-4, Changes; or FAR 52.243-5, Changes and Changed Conditions.

In addition to the above responsibilities, the COR and/or Contractor shall immediately notify the Contracting Officer of any contractual concerns related to the following:

Personal Services: FAR 37.104(a) provides that, "[a] personal services contract is characterized by the employer-employee relationship it creates between the Government and the contractor's personnel. The Government is normally required to obtain its employees by direct hire under competitive appointment or other procedures required by the civil service laws. Obtaining personal services by contract, rather than by direct hire, circumvents those laws unless Congress has specifically authorized acquisition of the services by contract."

Under this contract, the services to be performed do not require the Contractor or the Contractor's personnel to exercise personal judgement and discretion on behalf of the Government. Rather, the Contractor's personnel will act and exercise personal judgement and discretion on behalf of the Contractor. The services to be performed under this contract are not for personal services as defined by FAR 37.104.

Both the Government and the Contractor have a responsibility to monitor contract activities. The CO must be notified immediately if at any time during contract performance the interaction between the Government representative and Contractor personnel constitutes or is perceived to constitute personal services. Both the Government and Contractor personnel must exercise

caution to ensure that service contracts not personal in nature avoid even the appearance of a personal services contract.

Inherently Governmental Functions: The agency shall not use contractors for the performance of inherently governmental functions unless issued under statutory authority See FAR 7.5 Inherently Governmental Functions. As defined in FAR 2.101, "Inherently Governmental Function" means, as a matter of policy, a function that is so intimately related to the public interest as to mandate performance by Government employees. An inherently governmental function includes activities that require either the exercise of discretion in applying Government authority, or the making of value judgments in making decisions for the Government. Inherently governmental functions DO NOT normally include gathering information for or providing advice, opinions, recommendations, or ideas to Government officials.

FAR 7.503(c) provides a list of examples of functions considered to be inherently governmental functions or which shall be treated as such.

To this effect, during contract performance, care should be taken to ensure that any change or expansion in scope of the requirement does not include inherently governmental functions. Further, due to the nature of a given requirement, there is a potential for close working relationships to develop between Government and Contractor personnel; however, care should be taken to ensure that any familiarity established between the Government and Contractor personnel never promotes or fosters an environment that allows for the assignment of inherently governmental functions to contractor employee(s).

Unauthorized Commitments: In carrying out his/her duties, in accordance with FAR 1.602-2(d)(5), the COR "has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract, or in any way direct the Contractor, or its Subcontractors, to operate in conflict with the contract terms and conditions." Doing so constitutes an "unauthorized commitment." The Contracting Officer is the only individual with the authority to enter into an agreement on behalf of the Government. An unauthorized commitment is defined as "an agreement that is not binding solely because the Government representative who made it lacked the authority to enter into that agreement on behalf of the Government." FAR 1-602-3(a). Examples of unauthorized commitments include, but are not limited to, the following:

- Orders placed with a Contractor without a valid contractual instrument in place.
- Directing any Contractor to do additional work, in excess of the contract value, or work beyond the Period of Performance.
- Authorize new work to a contract without notifying the Contracting Officer (CO) or Contract Specialist (CS) and having a modification in place for the new work.
- Directing the Contractor, in any way that could change the terms and conditions of the contractual instrument or be deemed outside the Scope of the contract.

Unauthorized commitments are a serious matter and may result in personal liability on the part of the employee who committed the unauthorized commitment. Ratification, is "the act of

approving an unauthorized commitment by an official who has the authority to do so." FAR 1.602-3(a).

(end of clause)

H.1 CONFLICT OF INTEREST (OCT 2020)

a. General: The contractor and the services provided under this contract shall be free, to the greatest extent possible, of all Organizational and Personal Conflicts of Interest. Consistent with these terms and conditions, all references to Organizational and/or Personal Conflicts of Interests will be referred to individually or collectively, as Conflicts of Interest (COI). Except as defined by these terms and conditions and in accordance with FAR 9.503, the Contracting Officer shall not maintain a contract with a contractor the Contracting Officer (CO) determines has, or has the potential for, an unresolved COI.

b. Definitions:

Actual COI– The COI is either currently in existence as determined by the contractor or CMS. This form of COI will require avoidance, neutralization or mitigation acceptable to CMS.

Affiliates –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.

Apparent (Perceived) COI – The COI on first observation appears to be an actual or potential COI, but may or may not be after analysis.

Avoidance – To prevent the occurrence of a COI through actions such as exclusion of sources or modification of requirements. Avoidance precludes the conflict.

Contractor – The term contractor is used synonymously with offeror.

Financial Relationships – A direct or indirect ownership or investment interest (including a stock 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.

Mitigation– To reduce the effects of a COI to an acceptable level of risk so that the Government's interest with regard to fair competition and/or contract performance are not impaired. The conflict remains but action was taken that minimizes the impact of the conflict to an acceptable level of risk.

Mitigation Plan – The contractor's written approach to mitigating a COI as documented in an attachment to this order.

Neutralization – To counteract, through a specific action, the effects of potential or actual COI. The conflict remains, but the impact of the conflict has been negated.

Organizational Conflict of Interest – Occurs when 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.

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

Potential COI – A future situation or circumstance that would create a conflict of interest.

Three (3) Types of COIs include:

Conflict Types	Definitions
Biased Ground Rules	Consists of situations where a contractor and/or its affiliate(s), 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 entity could skew the competition, whether intentionally or not, in favor of itself and/or its affiliates.
Impaired Objectivity	Consists of situations where a contractor and/or its affiliate(s) has an interest (typically financial) that may conflict with the interest of the Government to whom the contractor has a contractual obligation, and where the entity's work under the Government contract could give the contractor the opportunity to benefit its other business interests. If the entity is providing recommendations, judgment or advice, and its other business interests could be affected by that recommendation, judgment or advice, it's objectivity may be impaired. An example is where the entity was evaluating itself or evaluating 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 where a contractor and/or its affiliate(s) 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 entity 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 contractor and/or its affiliates gaining an unfair competitive advantage; there is no issue of bias. Note: Incumbency alone does not constitute "unequal access to information."

c. Significant Potential Conflict of Interest:

1. Nature of Potential Conflict: Although not all inclusive, the Contracting Officer has determined that the following activities are considered to be an actual, potential or apparent COI with the work to be performed under this contract.

The contractor shall promptly notify the CO if it is an entity, or affiliated with an entity, where any of the following circumstances exist:

a. Biased Ground rules, impaired objectivity or unequal access to information as explained in the definitions above and/or;

b. Within the three types of conflicts of interest, the CO has identified the following specific circumstances of conflicts:

- Develop a system for which it wrote the requirements; or
- Develop a claims processing system for the Government and is affiliated or has a financial relationship, as these terms are explained above, with an entity that pays claims; or
- Design infrastructure under a systems development contract that it will be selling the Government under a hosting contract; or
- Provide security testing or other testing on a system that it developed; or
- Inspect deliverables on behalf of the Government that it submitted to the Government for inspection under a different contract.

2. Proposed Restraint on Future Contractor Activities: none

d. Conflict of Interest Oversight and Mitigation Plan:

1. Conflict of Interest Oversight Program: The contractor shall maintain an effective COI Oversight Program throughout the performance of the contract which includes procedures to monitor and disclose all Organizational and Personal Conflicts of Interest. A COI oversight program should include the monitoring of personal conflicts of interest such as, but not limited to:

a. Managers or Key Personnel who would be, or are involved with, the performance of this contract;

b. Governing Body Members (e.g., Board of Directors; Trustees); and

c. Principals of the organization as defined by FAR 52.203-13, Contractor Code of Business Ethics and Conduct.

2. Mitigation Plan: At any time during the performance of the contract if an actual, potential, or apparent COI is identified whether by the CO, the contractor or otherwise, the contractor shall submit a mitigation plan [See Delivery Order Attachment] within 30 days unless otherwise specified by the CO. It is the contractor's responsibility under the terms and conditions to provide timely notification to the CO those COIs that are self-identified. The CO will notify the

contractor regarding the specifics for submission. The Government will review the submission at which time a determination will be made whether a COI has been satisfactorily mitigated or if further action is necessary and will notify the contractor accordingly. In cases where a COI cannot be, or has not been, mitigated to the Government's satisfaction, the Government may take the following actions (this list is not all inclusive):

a. Request a waiver in accordance with FAR 9.503 Waiver, from the Head of the Contracting Activity;

b. Make changes to the requirements of the contract;

c. Require a subcontractor change (if the conflict lies with the subcontractor); and/or

d. Terminate the contract in whole or in part.

e. Subcontractor Flow-Down Terms and Conditions: The prime contractor is responsible for avoiding, neutralizing and mitigating all actual, potential, or apparent COIs of its subcontractors, in accordance with these terms and conditions. Therefore, the prime contractor shall flow-down this clause in all subcontracts. For subcontractors, wherever the term "contractor" is used, insert "subcontractor."

(end of clause)

H.2 CMS INFORMATION SECURITY (OCT 2020)

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 all Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS) and CMS Information Security requirements located at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Security-and-Privacy-Language-for-Procurements. 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 https://csrc.nist.gov/projects/risk-management. 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 https://www.gsa.gov/technology/government-it-initiatives/fedramp. 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-Security-and-Privacy-Language-for-Procurements.

(end of clause)

H.3 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.

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

(end of clause)

H.4. CMS SECURITY CLAUSE (MAY 2018)

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 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.

(end of clause)

H.5 Mandatory Contractor Training (JULY 2021)

All contractor employees who have access to (1) HHS Federal Information or a Federal information system or (2) personally identifiable information shall complete the CMS provided Records management training required by the Department of Health and Human Services (HHS) before performing any work under their contract. Thereafter, the employees must complete annual Records Management training throughout the life of the contract. The Contractor shall also ensure subcontractor compliance with this training requirement.

Link to the training can be found here: https://www.cms.gov/About-CMS/Contracting-With-CMS/ContractingGeneralInformation/Contracting-Policy-and-Resources

Contractor employees are expected to complete any new training requirements enacted by HHS, whereby access to the course material has been provided. These courses are at no additional cost to the contract and the contractor is not required to provide documentation on such training unless specifically requested. The Government does not anticipate a contractor will develop a system specifically designed to track and monitor such trainings, but will address the requirements under overall contract management and adherence to regulations as noted in the Contractor Performance Assessment Reporting System (CPARS).

(end of clause)

Appendix B: HHSAR and FAR Clauses

I.1 Department of Health and Human Services Acquisition Regulations (HHSAR) Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were provided in full text. Upon request, the Contracting Officer will provide the information in full text. The full text of a clause is also available electronically at http://www.hhs.gov/policies/hhsar/.

I.1 The following clauses are incorporated by reference:

352.203-70	Anti-Lobbying (DEC 2015)
352.208-70	Printing and Duplication (DEC 2015)
352.211-3	Paperwork Reduction Act (DEC 2015)
352.222-70	Contractor Cooperation in Equal Employment Opportunity Investigations (DEC 2015)
352.224-70	Privacy Act (DEC 2015)
352.224-71	Confidential Information (DEC 2015)
352.231-70	Salary Rate Limitation (DEC 2015)
352.232-71	Electronic Submission of Payment Requests (FEB 2022)
352.233-71	Litigation and Claims (DEC 2015)
352.239-70	Standard for Security Configurations (JAN 2010)
352.239-73	Electronic Information and Technology Accessibility Notice (DEC 2015)

(End of clause)

I.2 HHSAR 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.

The following individuals are considered as key personnel under this Delivery order:

Position Title	Name

(End of Clause)

I.3 HHSAR 352.239-74 Electronic and Information Technology Accessibility (DEC 2015)

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all electronic and information technology (EIT) supplies and services developed, acquired, or maintained under this contract or order must comply with the "Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR part 1194. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of Section 508 Final Provisions can be accessed at http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the Statement of Work or Specification or Performance Work Statement. The contractor must provide any necessary updates to the submitted HHS Product Assessment Template(s) at the end of each contract or order exceeding the simplified acquisition threshold (see FAR 2.101) when the contract or order duration is one year or less. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are: *All of them are potentially applicable – the VPAT(s) submission of the contractor should indicate which, if any, the contractor believes to be inapplicable.*

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS website: (http://www.hhs.gov/web/508 and). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite Delivery contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include EIT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed HHS Section 508 Product Assessment Template and any other

additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found at http://www.hhs.gov/web/508. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

I.4 FAR 52.252-2 -- Clauses Incorporated by Reference (Feb 1998).

This contract incorporates one or more clauses 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/these address(es): www.acquisition.gov.

FAR 52.203-12	Limitation on Payments to Influence Certain Federal Transactions (JUN 2020)
FAR 52.204-9	Personal Identity Verification of Contractor Personnel (JAN 2011)
FAR 52.204-14	Service Contract Reporting Requirements (OCT 2016)
FAR 52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (NOV 2021)
FAR 52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (NOV 2021)
FAR 52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (NOV 2021)
FAR 52.217-6	Option to Increase Quantity (MAR 1989)
FAR 52.219-14	Limitations on Subcontracting (OCT 2022)
FAR 52.222-54	Employment Eligibility Verification (MAY 2022)
FAR 52.227-14	Rights in Data – General (MAY 2014)
FAR 52.232-18	Availability of Funds (APR 1984)
FAR 52.243-7	Notification of Changes (JAN 2017)
FAR 52.244-2	Subcontracts (JUN 2020)
FAR 52.244-6	Subcontracts for Commercial Items (OCT 2022)

(End of clause)

I.5 FAR 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance

hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days prior to the end of the term of the order.

(End of clause)

I.6 FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within any point prior to the end of the term provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years.

(End of clause)

(End of Section I)