**The following clauses are incorporated in their entirety into the governing PO. Reference to "Contractor" hereinbelow shall refer to supplier, vendor, subcontractor or similar in the governing PO.**

1. **Access Restriction/Information Handling (H2)**

Contractor shall restrict access to information and facilities to those individuals with a valid need-to-know who are actually providing services under this contract. Further dissemination of information to other contractors, subcontractors, or other government agencies and private individuals or organizations is prohibited unless authorized in writing by CenturyLink. As requested by CenturyLink, Contractor shall require its employees performing work on this contract and subcontractors to sign a government specific Non-Disclosure Agreement. Contractor shall also require its subcontractors to sign corporate and individual non-disclosure agreements.

2. **Non-Personal Services (H6)**

As stated in the Federal Register, Volume57, No. 190, page 45096, dated September 30, 1992, Policy Letter on Inherently Governmental Functions, no personal services shall be performed under this contract. No Contractor employee will be directly supervised by the Government. All individual employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, Contractor shall promptly notify the CO of this communication or action.

Contractor shall not perform any inherently governmental actions under this contract. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, Contractor employee shall state that they have no authority to in any way change the contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.
Contractor shall ensure that all of its (and subcontractor) employees working on this contract are informed of the substance of this clause. Nothing in this clause shall limit the Government's rights in any way under any other provision of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this clause shall be included in all subcontracts at any tier.

**3. Contractor Security Personnel (H-7)** As part of its duties and obligations under this contract, the Contractor shall adhere to all applicable directives, instructions, orders, regulations and manuals that provide for the security of SCI and classified information including, but not limited to, the following:

- (U) Executive Order 12829 (establishing the National Industrial Security Program (NISP));
- (U) Director Central Intelligence Directives (DCID) 6/1, 6/3,DCID 6/6, DCID 6/7, and DICD 6/9;
- (U) Intelligence Community Directives (ICD) 503, 701, 704;
- Department of Defense (DoD) National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M; and DoD NISPOM Supplement (DoD 5520.22-M-Sup 1); and

All other applicable directives, instructions, orders, regulations and manuals not specifically identified herein which provide the necessary security & classification guidance for personnel, information, physical, Automated Information Systems, (AIS), and technical security measures.

Inquiries pertaining to SCI classification guidance determination or interpretation shall be directed to the CenturyLink CSSO. The Contractor shall identify and appoint (in writing) security personnel or representative(s) (hereafter referred to as Contract Special Security Officer(s) (CSSO) and Contract Special Security Representative(s) (CSSR) under this contract. CSSO and CSSR appointment correspondence shall include and identify specific facilities and/or projects to which security appointees are assigned. Copies of appointment letters shall be provided to the CenturyLink CSSO. CSSO appointees shall ensure that the transmission, handling storage, discussion, and processing of SCI is conducted in accordance with all applicable security directives, instructions, order, regulations and manuals, including, but not limited to those specifically identified above, and in accordance with all other terms and conditions of this contract. Supplemental security guidance from the CenturyLink Security Officer will be provided to the Contractor as required.

**4. Access to and Protection of Classified Information (H-8.2)**

Performance on this contract may require Contractor to gain access to classified National Security Information (includes documents and material), which mandates protection in accordance with Executive Order 13526, National Security Information (NSI), as amended, as well as any supplemental directives. Performance on this contract will require the contractor to have access to COMSEC material for the utilization of a STE phone device to be located in the government approved secured facility..

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification (an attachment in the contract); the National Industrial Security Program Operating Manual (NISPOM), as well as any relevant Intelligence Community Directives (ICDs) for protection of classified and/or compartmented information at its cleared facility, if applicable, or as further directed by the CenturyLink Special Security Officer (SSO). If the Contractor is required to have access to classified information at any DHS or other Government facility, it shall abide by the security requirements set forth by the Cognizant Security Authority (CSA) for that facility.

**5. Non-Personal Services (H-9)**

No personal services shall be performed under this contract. No Contractor employee will be directly supervised by the Government. All individual employee assignments and daily work directions shall be given by the applicable employee supervisor. If Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, Contractor shall promptly notify the CenturyLink Program Manager of this communication or action.

Contractor shall not perform any inherently governmental actions under this contract. No Contractor employee shall hold him or herself out to be a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communication with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work for. In all communication with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change the contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the CenturyLink Program Manager for that contract and not carry out the direction until a clarification has been issued by them.

The substance of this clause shall be included in all subcontract at any tier.

**6. Safeguarding of Sensitive Information (MAR 2015) (H-10)**

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by CenturyLink Program Manager or CSSO.

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by CenturyLink Program Manager or CSSO.

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1)Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3)Citizenship or immigration status

(4)Ethnic or religious affiliation

(5)Sexual orientation

(6)Criminal History

(7) Medical Information

(8)System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the CenturyLink Program Manager or CSSO.

(d) *Handling of Sensitive Information*. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook,* DHS 4300B DHS National Security Systems Policy Directive, and DHS 4300C Sensitive Compartmented Information (SCI) Systems provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures,

program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. Contractor shall provide copies of the signed NDA to the CenturyLink Program Manager or CSSO. no later than two (2) days after execution of the form.

(4) Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII.

(e) (U) *Authority to Operate*. Contractor shall not input, store, process, output, and/or transmit sensitive information within a CenturyLink IT system without an Authority to Operate (ATO) signed by the CenturyLink Program Manager or CSSO. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the CenturyLink Program Manager or CSSO within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the CenturyLink Program Manager or CSSO. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2)If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, *DHS 4300B DHS National Security Systems Policy Directive*, and *DHS 4300C Sensitive Compartmented Information (SCI) Systems*; Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the CenturyLink Program Manager or CSSO.
(2) (U) The Contractor shall provide full access and cooperation for all activities determined by the CenturyLink Program Manager or CSSO to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
(3) Incident response activities determined to be required by the CenturyLink Program Manager or CSSO. may include, but are not limited to, the following:
(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.
(4) The CenturyLink Program Manager or CSSO may be directed by the Government, at its sole discretion, to obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the CenturyLink Program Manager or CSSO. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the CenturyLink Program Manager or CSSO, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the CenturyLink Program Manager or CSSO, has determined in writing that notification is appropriate.

(2) Subject to CenturyLink Program Manager or CSSO analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the CenturyLink Program Manager or CSSO.

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the CenturyLink Program Manager or CSSO. ; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the CenturyLink Program Manager or CSSO following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

**7. Information Technology Security and Privacy Training (MAR 2015) (H-11)**

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor").

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The CenturyLink PM and CSSO requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the CenturyLink PM or CSSO not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the CenturyLink PM or CSSO not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the CenturyLink PM or CSSO via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.