AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGES
QP0022174	1		8

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00125	See Block 16B	PR201707240005	

6. ISSUED BY CODE

General Services Administration/FAS/ITC
Office of Acquisition Operations
1800 F Street, NW, 3rd Floor
Washington DC 20405
Andrea Lane
703-306-6825

7. ADMINISTERED BY *(If other than Item 6)* CODE

8. NAME AND ADDRESS OF CONTRACTOR

Qwest Government Services, Inc. dba CenturyLink QGS DUNS #178617031
4250 Fairfax Drive
Arlington, VA 22203-1665

CODE FACILITY CODE

( ) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED ***(SEE ITEM 11)***

X 10A. MODIFICATION OF CONTRACT/ORDER NO.

GS00Q17NSD3006

10B. DATED ***(SEE ITEM 13)***

7/31/2017

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is ☐ extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning ___ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATA SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

( ) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

X C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
Mutual Agreement of Both Parties (FAR 43.103(a)(3))

OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor _ is not, X is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

SEE CONTINUATION PAGES

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
Michael Glazer Federal Contracts Manager	Andrea Lane Contracting Officer
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
Michael Glazer	4-13-20	ANDREA LANE	Digitally signed by ANDREA LANE Date: 2020.04.13 10:24:40 -04'00'

PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 11/2016)
Prescribed by GSA
FAR (48 CFR) 53.24

1. The purpose of this modification is to incorporate CenturyLink's Submission Number CL00189.02a dated October 3, 2019, into the CenturyLink Enterprise Infrastructure Solutions (EIS) contract. The submission is proposing to add updates to Section 2.8.4 Managed Trusted Internet Protocol Service:

    - Two additional TIC Portal locations in Englewood, CO and Burbank, CA
    - SOC relocation from Columbia, MD to Foxborough, MA
    - Additional updates related to Trusted Internet Connections (TIC) Reference Architecture Document Version 2.2 (Section C.2.8.4.1.2 Standards).
    - Additional updates related to EIS Contract Modification P00004:
        - Modified Section C.1.8.8 to add Items 4-7
        - Modified the diagram in Section C.2.8.4.1.1.s to remove Sensitive Compartmented Information Facility (SCIF) from the diagram
        - Deleted Section C.2.8.4.1.4.1
        - Modified Section C.2.8.9.1.4, Item 30 to read "Provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details to be provided with DHS Task Orders."
    - Updates to statements regarding CenturyLink's SSP to reflect current status:
        - "CenturyLink's SSP has been accepted by GSA since 2010 and by DHS since its first audit in 2010. As of February, 2019, our MTIPS SSP complies with NIST SP 800-53 Revision 4 and is delivered to GSA at least annually with system updates."
        - "CenturyLink structures the SSP in accordance with the latest revision of NIST SP 800-18 and other relevant NIST and GSA guidelines. Our SSP includes appendices that include required policies and procedures across 18 control families mandated per FIPS 200. Our MTIPS SSP is maintained and updates are regularly delivered at least once per year, along with the monthly Plan of Action and Milestones (POA&M) reports as appropriate."
- Updates to Section 1.4.8.8.4 DIPSS Technical Capabilities related to EIS Contract Modification P00004:
    - Addition of Item 30 to Figure 1.4.8.8.4-1 DIPSS Technical Capabilities:
        - "CenturyLink will provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details will be based on DHS Task Orders."

The following changes are proposed:

1) Page 1-204, Section 1.4.8.1 paragraph 1 and 2, are changed to the following:

1.4.8.3.1 Understanding (L.29.2.1-A; M.2.1-1)

CenturyLink's MTIPS is based upon a network architecture (see ***Figure 1.4.8.3.1-1***) that is fully capable of meeting each of the DHS' 74 TIC 2.2 requirements. Our solutions deliver high availability through a redundant architecture: TIC Portals (located in Sterling, Virginia; Chicago, Illinois; Englewood, CO; and Burbank, CA); SOCs (located in San Diego, California, and Foxborough, MA); NOCs (located in Arlington, Virginia, and St. Paul, Minnesota); portal-to-MPLS connections; portal-to-Internet dedicated edge

(DE) connections; MPLS PE to private core (PCOR) connections; and access options with diversity for automatic failover.

CenturyLink's MTIPS provides agencies with numerous key features and benefits as highlighted in ***Table 1.4.8.3.1-1***.

2) Page 1-205, Section 1.4.8.3.1, second paragraph is changed to the following:

CenturyLink's MTIPS and web interfaces are engineered to provide high availability through the use of redundant network connections, assets, and operation centers. Subscribing agencies will be afforded a solution with capabilities offering the protection of the core security services of MTIPS to include managed firewall service (MFS), intrusion detection and prevention service (IDPS), antivirus management service (AVMS), email scanning and archiving, DNS logging, and full packet capture (FPC) functions. ***Figure 1.4.8.3.1-1*** depicts the CenturyLink MTIPS TIC 2.0 architecture.

3) Page 1-206, Section 1.4.8.3.1, paragraph 1 is changed to the following:

Inspection and Filtering

CenturyLink's firewall appliances are located within the four MTIPS TIC portals to provide stateful inspection, filtering, blocking, and alerting of all inbound and outbound agency IPv4/IPv6 traffic and protocols such as ICMP, TCP, and UDP protocols. This creates a defense-in-depth security framework and provides a layered inspection and filtering solution enabling individual packet inspection and admission based on an agency's policy. CenturyLink's MTIPS solution includes the following firewall and proxy service features:

4) Page 1-206, Section 1.4.8.3.1 Table is changed to the following:

CenturyLink Service Highlights—MTIPS
✦ MTIPS provider since 2010
✦ Existing MTIPS architecture is TIC 2.2 compliant
✦ Existing MTIPS service ranges from T1 to 10Gbps connections
✦ Four geographically diverse TIC Portals

- TIC Portal throughput scalable to 40 Gbps
- Route diversity or avoidance on the POP-to- SDP network segment to increase site and service survivability
- 24x7x365 NOC and SOC monitoring and management of EIS subscriber circuits, services, and service termination equipment

5) Page 1-208, last paragraph is changed to the following:

Domain Name Service

CenturyLink will provide a managed external DNS infrastructure service that is responsive, robust, and secure both for agency personnel to reach the Internet and the general public to reach the agency's public facing services to deliver the best security characteristics per the DHS TIC Reference Architecture. CenturyLink's DNS service includes four elements: authoritative servers, recursive servers (caching), DNSSEC, and filtering that provides TIC reference architecture best practices and the security controls to meet NIST SP 800-81 revision 2, as authorized in our MTIPS System Security Plan (SSP) (as originally developed for Networx).

6) Page 1-212, Section 1.4.8.3.1.1, last paragraph is changed to the following:

CenturyLink's MPLS/VPNS transport network will serve as a secure collection point for virtual or physical TIC connectivity by enabling the termination of MTIPS access connections to MPLS PE routers. Private virtual route forwarding (VRF) or closed user group (CUG) instances will be provisioned on the CenturyLink MPLS transport network to isolate an agency's internal network traffic from other agency's MTIPS or VPNS user traffic to include Internet and external networks originated or terminated traffic.

7) Page 1-214, Section 1.4.8.3.1.1, first paragraph is changed to the following:

CenturyLink's MTIPS portals will function as an OMB-approved multi-service TICAP capable of hosting multiple agencies using VDOMs and CenturyLink's UTM platform that is capable of managing and correlating multiple independent traffic streams for each subscribing agency.

8) Page 1-214, Section 1.4.8.3.1.1, third paragraph is changed to the following:

CenturyLink has engineered and installed four geographically diverse domestic MTIPS TIC Portals in Sterling, Virginia; Chicago, Illinois; Englewood, CO; and Burbank, CA, that serve as secure Internet exchange points to subscribing departments/agencies.

9) Page 1-214, Section 1.4.8.3.1.1, fifth paragraph is changed to the following:

CenturyLink will work with an agency to implement virtual TIC capabilities (as defined in agency TO), to agencies with resources hosted outside their physical boundaries.

10) Page 1-214, Section 1.4.8.3.1.1, last paragraph is changed to the following:

The SOC systems providing management and monitoring of the MTIPS TIC Portals will be dedicated for the use of government entities and will be isolated from non-government/commercial systems. ***Figure 1.4.8.3.1-2*** shows CenturyLink's high-level overview of the SOC management process and systems.

11) Page 1-217, Section 1.4.8.3.1.4.1 remove the following:

C.2.8.4.1.4.1 (#4) CenturyLink currently has ICD 705 accredited space for MTIPS adjacent to, but logically separate from, the SOC, CenturyLink provides two or more TS/SCI cleared SOC personnel that are available 24x7x365 and who will respond within two hours of notification to handle secure communications (e.g., voice, email) in the managed secure space with authority to report, acknowledge, and initiate action based on TS/SCI-level information, including tear line information, with US-CERT. CenturyLink currently has both a primary and alternate DHS accredited SCIF, in which to accommodate a DHS-provided Secure Terminal Equipment (STE), secure FAX, and DHS secure network equipment in order to support the rapid response loop requirements.

12) Page 1-219, Section 1.4.8.3.1.4.2, first paragraph is changed to the following:

CenturyLink's MTIPS provides the following MTIPS transport collection and distribution capabilities: CenturyLink operates two TIC Portals: Sterling, Virginia; Chicago, Illinois; Burbank, CA; and Englewood, CO. Agency's Internet bound or sourced traffic will be processed by one of the TIC Portals.

13) Page 1-219, Section 1.4.8.3.1.4.2, second paragraph is changed to the following:

CenturyLink creates an agency trusted domain (DMZ) in one of two ways (encrypted DMZ (eDMZ) and inner firewall):
An eDMZ, a router-based security solution, ensures that an agency's traffic is protected and physically isolated when transported to the TIC Portal and the public Internet. In an eDMZ deployment, an IPSec/VPN tunnel is established between a FIPS 140-2 compliant router at the agency SDP and the firewall within the TIC Portal.
An inner firewall is deployed by two options: 1) an IPSec/VPN tunnel between a FIPS 140-2 compliant firewall at the agency SDP and the firewall within the TIC Portals or 2) a pseudo-wire (layer 2) VPN tunnel between the agency termination point on CTL MPLS and the MTIPS gateway PE.

Both DMZ approaches provide the necessary security from the agency SDP over the MTIPS access circuit and transport network to the TIC Portal, thus ensuring the agency traffic is not sniffable, and ports cannot be spoofed.

14) Page 1-223, Section 1.4.8.3.2 Quality of Service, first paragraph is changed to the following:

CenturyLink was the first MTIPS provider to complete the TCV and to receive an ATO from GSA in 2010. CenturyLink has consistently maintained a 100% score during the annual DHS US-CERT TCV assessment for all of the critical and mandatory capabilities. MTIPS is a premiere core security service, and CenturyLink is dedicated and committed to maintaining MTIPS compliance and our ATO as security requirements evolve to address the ever-changing threat vectors focused upon the government.

15) Page 1-225, Section 1.4.8.3.3 MTIPs Service Coverage, second to last paragraph is changed to the following:

CenturyLink operates four MTIPS TIC portals for EIS located in Chicago, Illinois; Sterling, Virginia; Burbank, CA and Englewood, CO; with SOCs in San Diego, California, and Foxborough, MA. CenturyLink MNS will be available at all locations where the underlying CenturyLink EIS services are provided.

16) Page 1-229, Section 1.4.8.3.4.4 System Security Plan, second paragraph is changed to the following:

CenturyLink's SSP has been accepted by GSA since 2010 and by DHS since its first audit in 2010. As of February, 2019, our MTIPS SSP complies with NIST SP 800-53 Revision 4 and is delivered to GSA at least annually with system updates.

17) Page 1-229, Section 1.4.8.3.4.4 System Security Plan, fourth paragraph is changed to the following:

1. CenturyLink structures the SSP in accordance with the latest revision of NIST SP 800-18 and other relevant NIST and GSA guidelines. Our SSP includes appendices that include required policies and procedures across 18 control families mandated per FIPS 200. Our MTIPS SSP is maintained and updates are regularly delivered at least once per year, along with the monthly Plan of Action and Milestones (POA&M) reports as appropriate.

18) Page 1-230, Section 1.4.8.3.4.4 System Security Plan, first paragraph is changed to the following:

2. As required by the GSA, the CenturyLink SSP will include the Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37 to specify the actual security assessment boundary (also referred to in this proposal as the "A&A boundary") and components within the information system. The initial boundary, and subsequent changes to it, will be a cooperative effort between the federal government and CenturyLink Information System Owners, Chief Information Security Officers, the GSA Authorizing Official, and Information Systems Security Manager/Officer. Our initial EIS BSD, which is based on our currently approved Networx BSD, will be completed and submitted within 15 days of the NTP.

19) Page 1-287 insert into last entry of Figure 1.4.8.8.4-1 DIPSS Technical Capabilities:

✓	30.	• CenturyLink will provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details will be based on DHS Task Orders.

3. The estimated dollar value of the contract remains unchanged.

4. Except as provided herein, all prices, terms and conditions of the document referenced in Item 10A remain unchanged and in full force and effect.