CENTURYLINK

DRAFT NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (NS/EP)

DRAFT

CDRL 83

November 4, 2016

Qwest Government Services, Inc. dba CenturyLink QGS

4250 N Fairfax Drive, Suite 300

Arlington, VA 22203

REVISION HISTORY

Revision Number	Revision Date	Revision Description	Revised by

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (G.11)

Providing for the continuity of critical national security and emergency preparedness (NS/EP) communications is vital to CenturyLink's history of comprehensive and progressive planning to ensure that CenturyLink continues to meet the United States Government's expectations for continuity of service.

CenturyLink's NS/EP program is an integral part of its corporate risk management strategies and procedures and is supported at the highest levels of the corporation. CenturyLink works with the government to ensure that the necessary policies, plans, and operational response protocols are in place to fulfill NS/EP responsibilities and obligations for both day-to-day activities and long-term contingency planning.

Kathryn Condello, CenturyLink's Director of National Security and the director for NS/EP, is based in the National Capital Region (NCR) and physically resides in the Department of Homeland Security (DHS) National Coordinating Center (NCC) and National Cybersecurity and Communications Integration Center (NCCIC). Executive Orders (EO) 12472 and 13618 and their successors will be considered in the design and operation of services provided under this contract.. CenturyLink's CEO Glen Post is a current member of the President's National Security Telecommunications Advisory Committee (NSTAC) (see ***Figure 1*** below). As past NSTAC chairman, he has had ongoing membership and various leadership roles in both the Communications Sector Coordinating Council and the Communications Information Sharing and Analysis Center, where many of the planning and exercises for procedures, policies, standards and operational response efforts are undertaken. The Director of NS/EP is on-call 7x24 through the DHS NCC for general inquiries and represents CenturyLink in responding to status inquiries during an event supporting DHS/Federal Emergency Management Agency (FEMA) in Emergency Support Function #2 which states:

"Emergency Support Function (ESF) #2—Communications supports the restoration of the communications infrastructure, facilitates the recovery of systems and applications from cyber attacks, and coordinates Federal communications support to response efforts during incidents requiring a coordinated Federal response."
FEMA.gov Media Library

Figure 1. CenturyLink's CEO Glen Post seated fourth from the left of President Barack Obama. May 6, 2015 NSTAC Meeting. The White House.

Ms. Condello is a member of the Cyber Unified Coordinating Group, as reflected in the National Cyber Incident Response Plan.

Mr. Post served as the past chair and is a current member of the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council.

CenturyLink ensures that critical government and industry needs are met when an actual or potential emergency threatens national security or its socioeconomic structure. As part of this plan, CenturyLink will continue to ensure compliance with NS/EP related policy directives specified in RFP Section G.11 through its NS/EP Functional Requirements Implementation Plan, including annual updates, pursuant to the requirements set forth in RFP Sections G.11.1 through G.11.3, as addressed below in Sections 1 through 3, and will immediately notify the government when events arise that may have major consequences to its network and EIS services. This notification is similar to the "abnormal report" currently furnished to the NCC and NCCIC. While the

GSA contracting officer (CO) will set priorities, CenturyLink will be solely responsible for network operations.

1.0 BASIC FUNCTIONAL REQUIREMENTS (G.11.1)

As shown in ***Table 1.0-1***, for its awarded services and core based statistical areas (CBSAs), CenturyLink will support the 14 basic functional requirements for NS/EP telecommunications and IT services, as identified by the DHS OEC and the Office of Science and Technology Policy (OSTP).

Table 1.0-1. Functional Requirements

Approach to Satisfy NS/EP Functional Requirements (RFP Section G.11.1)		
NS/EP Functional Requirements		***CenturyLink Approach***
1. Enhanced Priority Treatment	Voice and data services supporting NS/EP missions have priority over other traffic	[redacted]
2. Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.	[redacted]
3. Non-Traceability	Select users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).	[redacted]

Approach to Satisfy NS/EP Functional Requirements (RFP Section G.11.1)		
NS/EP Functional Requirements		***CenturyLink Approach***
4. Restorability	Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.	[redacted]
5. International Connectivity	Voice and data services must provide access to and egress from international carriers.	[redacted]
6. Interoperability	Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks that will be identified after contract award.	[redacted]
7. Mobility	Voice and data infrastructure must be in place to support transportable, re-deployable, or fully mobile voice and data communications (e.g., personal communications service (PCS), cellular, satellite, and high-frequency (HF) radio).	[redacted]
8. Coverage	Voice and data services must be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.	[redacted]
9. Survivability/ Endurability	Voice and data services must be robust to support users in a broad range of circumstances, from natural or manmade disaster to nuclear war.	[redacted]
10. Voice Band Service	Voice band service must be provided in support of presidential communications.	[redacted]

Approach to Satisfy NS/EP Functional Requirements (RFP Section G.11.1)		
NS/EP Functional Requirements		***CenturyLink Approach***
11. Broadband Service	Broadband service must be provided in support of NS/EP missions (e.g., voice, imaging, web access, and multimedia).	[redacted]
12. Scalable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.	[redacted]
13. Affordability	The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).	[redacted]
14. Reliability/ Availability	Services must perform consistently and precisely according to their design requirements and specifications and must be usable with high confidence.	[redacted]

2.0 PROTECTION OF CLASSIFIED AND SENSITIVE INFORMATION (G.11.2)

CenturyLink may be granted access to certain classified and sensitive materials required for the planning, management and operation of NS/EP in support of EIS services. This information may be in various forms including hardcopy and softcopy. To ensure the protection of classified and sensitive information, CenturyLink will abide by agency-issued DD254s in support of EIS classified requirements through its government security organization. The CenturyLink Government security team of 30 security professionals is led by the Director of Industrial Security, Kent Geerlings, who is responsible for implementing the proper policies and procedures to meet the security requirements of all customers. [redacted] Mr. Geerlings has more than thirty years experience in dealing with various government entities and reports directly to our Corporate Vice President/Chief Security Officer, David Mahon, as shown in ***Figure 2.0-1***. This reporting structure ensures any potential security challenges are promptly resolved at a corporate level providing immediate and effective action.

Figure 2.0-1. CenturyLink Security Operations.

The CenturyLink's physical security program is responsible for our secure facilities beginning with construction planning through accreditation plans and final approvals and maintenance to ensure they are built and maintained according to the contractual requirements contained in the National Industrial Security Program Operating Manual (NISPOM) and Director of National Intelligence, Intelligence Community Directive (ICD) 705. CenturyLink currently has fifteen secure facilities located throughout CONUS.

Our information systems security personnel are responsible for our classified computer systems beginning with system design through accreditation plans and final approvals and maintenance to ensure they are built and maintained according to the contractual requirements contained in the NISPOM and Director of National Intelligence, ICD 503. These information security professionals successfully led the effort to accredit the systems for CenturyLink's MTIPS offerings under Networx and the systems for the

Networx Portal. CenturyLink currently has numerous accredited classified systems located throughout CONUS.

3.0 DEPARTMENT OF HOMELAND SECURITY OFFICE OF EMERGENCY COMMUNICATIONS PRIORITY TELECOMMUNICATIONS SERVICES (G.11.3)

CenturyLink will continue to comply and interoperate with, and provide all DHS Office of Emergency Communications (OEC) (formerly NCS) priority telecommunications services including TSP, GETS, wireless priority service (WPS), and, when released, next-generation network priority services (NGN-PS).

3.1 GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE (GETS) (G.11.3.1)

GETS is a White House-directed emergency telephone service provided by the DHS OEC to meet NS/EP requirements for the use of public, defense, or federal telephone networks by federal, state and local government and other authorized users.

GETS provides emergency access and specialized processing in local and long-distance telephone networks. GETS access is provided through a simple dialing plan and personal identification number (PIN). GETS traffic receives priority treatment over normal traffic through:

- Controls such as trunk queuing, trunk sub-grouping, or trunk reservation
- Exemption from restrictive network management controls that are used to reduce network congestion
- High probability of completion (HPC) capability to provide connectivity
- NS/EP identification
- Priority signaling

These features enhance the probability of NS/EP calls to be completed in congested networks. GETS does not preempt public traffic nor are there levels of precedence. GETS cards for authorized CenturyLink personnel are maintained Ms. Condello as the director for NS/EP, who provides cards when required and maintains accountability

records. Cards are provided only to individuals who have a need to circumvent the standard telecommunications process due to a qualified emergency situation.

CenturyLink will fully comply and interoperate with the GETS service. CenturyLink has local exchange carrier (LEC) and incumbent LEC (ILEC) agreements with established carriers for access purposes. We will add agreements for additional local access and business relationships as appropriate. The coupling of CenturyLink's network with the additional local access capabilities creates a shared network environment that will allow for excellent performance of GSA EIS services.

3.2 WIRELESS PRIORITY SERVICE

This requirement is not applicable to CenturyLink, as we have no wireless networks.

3.3 TELECOMMUNICATION SERVICE PRIORITY (TSP) (G.11.3.3)

CenturyLink uses TSP to provide restoration services supporting agencies that have obtained priority from the DHS OEC in the event of network degradation or failure. CenturyLink has been a provider of these services since the program's inception and has significant experience provisioning qualified TSP circuits for the government. The CenturyLink TSP program is overseen by the Director of NS/EP and managed by the CenturyLink risk management disaster preparedness organization, which ensures that CenturyLink meets all the mandated requirements of the TSP program. CenturyLink is a member of the DHS TSP oversight committee. CenturyLink provides priority provisioning (emergency and essential) and priority restoration services.

3.4 TSP PROVISIONING SERVICES

As shown in ***Figure 3.4-1***, this process covers the actions taken to properly provision service orders with TSP assignments containing provisioning priority. The CenturyLink TSP coordinator is the focal point for installation and concentrates CenturyLink's efforts on these activities as the top priority.

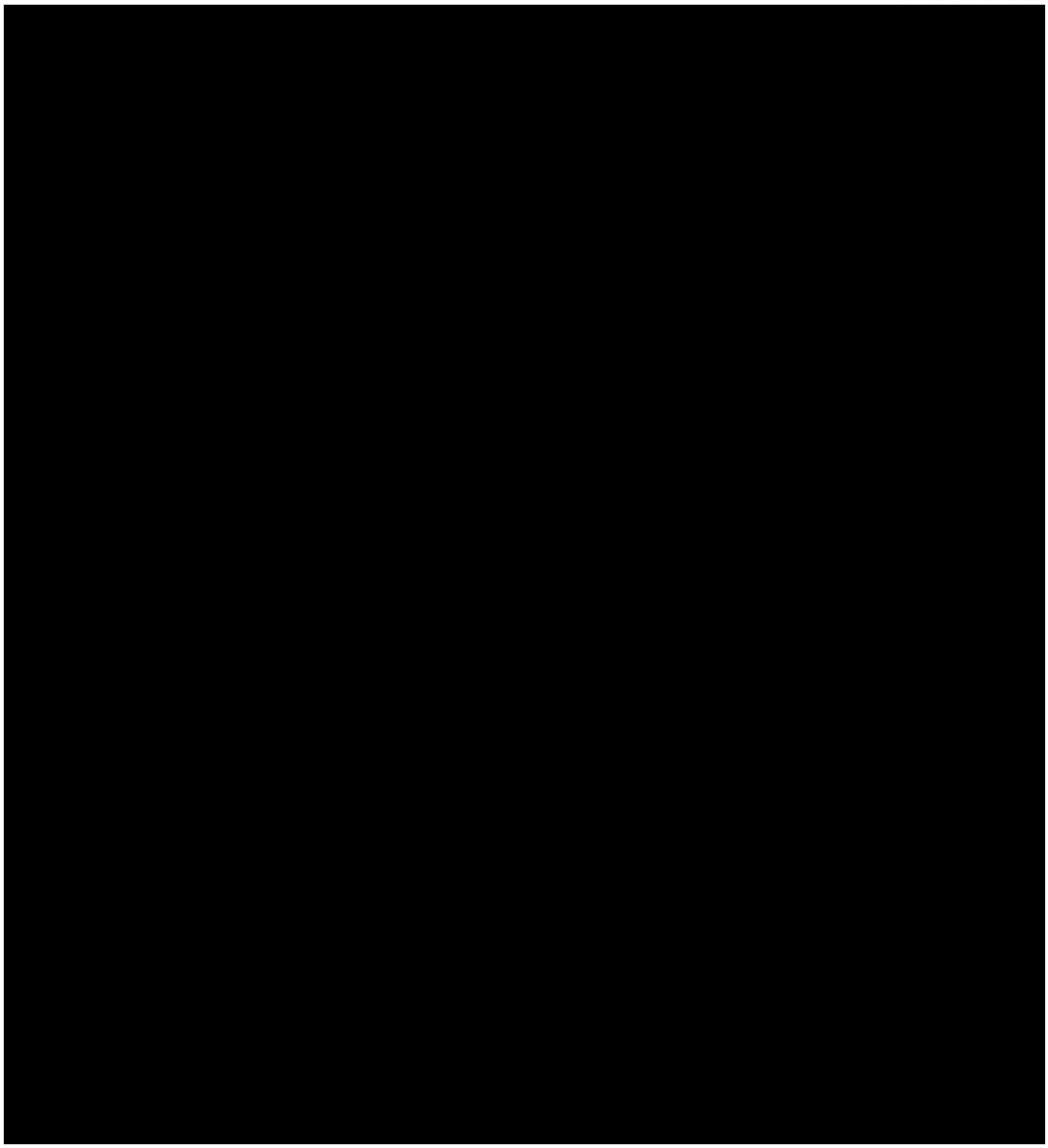

Figure 3.4-1. TSP Provisioning Process

The TSP provisioning process incorporates three key differences from CenturyLink's normal provisioning process:

1. **NS/EP**. New telecommunications services in the NS/EP category are so critical that they require provisioning at the earliest possible time, without regard to the cost
2. **Essential Provisioning.** This satisfies a requirement for a new service that must be installed by a specific date and cannot be delivered using normal business procedures

3. **Restoral of TSP Services.** CenturyLink adheres to strict guidelines set forth in the FCC report and order in prioritizing dispatch of maintenance personnel in response to customer reports

CenturyLink has maintained its compliance with the TSP program and will continue to do so for any future replacement system providing TSP services.

3.5 Restoration of Critical TSP Services

Restoration of critical TSP services covers the activities undertaken to properly restore service orders with TSP assignments containing restoration priority. The restoration of these services follow many of the normal steps of service restoration in that trouble tickets are created, CenturyLink's Customer Support Office (CSO) manages the restoration, and customers are provided updates. The key difference for TSP restoration of services is that CenturyLink restores TSP circuits before any other services. In cases where multiple circuits are down, services with TSP assignments are restored first and in the order of the TSP restoration priority.

CenturyLink complies with all applicable requirements in NCS Directive (NCSD) 3-1 (TSP System for NS/EP) and NCS Manual 3-1-1 (Service User Manual for the TSP System). This process covers all actions taken to:

- Manage the service order installation of services with TSP provisioning priority
- Manage the service order installation of services with TSP restoration priority
- Manage the restoral of services with TSP restoration priority

In meeting applicable requirements, the primary objectives of CenturyLink's management and restoration processes are to:

- Initiate service of orders with TSP provisioning priority within the designated time period
- Ensure all LECs meet the applicable TSP requirements
- Accurately capture and maintain the TSP information by circuit
- Properly restore services with TSP restoration priorities before services without TSP restoration priorities
- Properly restore services with TSP restoration priorities in order of priority

- Ensure that all required communications to OEC and customers occur in a timely and accurate fashion

In provisioning circuits on a TSP basis, CenturyLink's Program Management Office (PMO) will coordinate closely with the government PMO and ensure that instructions are followed and service requirements are met. CenturyLink's TSP coordinator will review the status of all TSP service orders with the CenturyLink PMO.

CenturyLink revalidates all TSP authorization codes every three years.