CENTURYLINK
DRAFT SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN

DRAFT

CDRL 77

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

1.0 SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN (L.29.1.2; G.6.3)

CenturyLink uses a Supply Chain Risk Management (SCRM) process that begins with procurement source selection strategy and supplier qualification and ends with proper disposition of equipment and completion of services provided to the government. CenturyLink's network design and engineering organization delivers solutions that incorporate equipment that has been properly vetted through its procurement channel either during source selection or through CenturyLink's pre-approved government and original equipment manufacturer (OEM) qualified resellers. CenturyLink does not directly manufacture or assemble equipment below the sub-component level. Our SCRM process flows down to our subcontractors including Enterprise Infrastructure Solutions (EIS) subcontractors pursuant to Request for Proposal (RFP) Section G.6.3. The National Institute of Science and Technology (NIST) Special Publication (SP) 800-161, SCRM for Federal Information Systems, issued April 2015, details the comprehensive approach to manage supply chain risks for agencies. CenturyLink has developed a SCRM plan, based on the CenturyLink information security policy that describes the necessary steps to protect the supply chain in accordance with the NIST SP 800-53 Rev 4, Control Requirement, and its supplemental guidance.

Approved suppliers (certified) have the appropriate quality control measures to prevent counterfeit items of being introduced into the supply chain

- Approved shipping methods
- Shipped in tamper-resistant packaging
- Controlled in all phases using electronic bar coding (which tracks movement, provides lifecycle, recurring inventory)
- Secure storage (with limited access)
- Equipment only handled by authorized personnel)
- Replacement equipment to be purchased from approved suppliers

Our SCRM Plan is aligned with the requirements set forth in RFP Section G.6.3. As discussed in Section 1.1, CenturyLink applies the General Services Administration

(GSA) five-phase process to ensure that we use only approved, validated and verified hardware and software for all CenturyLink EIS-supported solutions. CenturyLink will submit annual updates to the SCRM Plan to the EIS CO and appropriate CORs.

In support of the GSA Networx Universal and Enterprise contracts, CenturyLink has delivered SCRM plans for the Managed Trusted Internet Protocol Service (MTIPS) trusted Internet connection (TIC) Networx modification. Building on the foundation of CenturyLink processes and controls previously used to reduce supply chain risk, we have developed a draft EIS SCRM plan that consolidates our practices, standards, framework, process capabilities, and SCRM tools.

Figure 1.0-1 is CenturyLink's SCRM process framework that summarizes our guidance to ensure that all CenturyLink organizations follow the processes found in the NIST requirements. Being acutely aware of today's hardware and software vulnerabilities, CenturyLink is committed to providing a secure IT infrastructure free of external threats to the government and commercial customers.

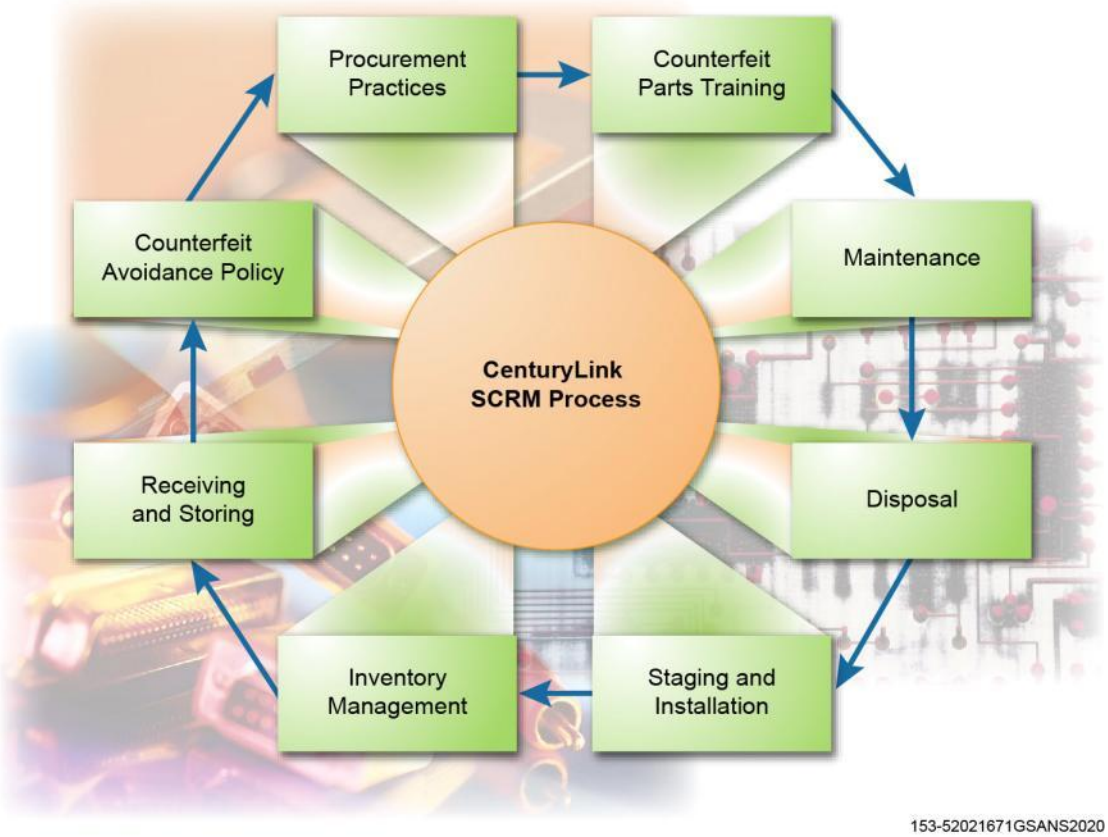

Figure 1.0-1. CenturyLink's Genuine Information Technology Tools (ITT) Lifecycle SCRM Framework

Meeting the requirements that will be applied to EIS task orders (TOs), CenturyLink's established SCRM process is used today to support the Networx MTIPS product and a series of other Federal Government programs. ***Figure 1.0-2*** is a flow diagram that portrays the CenturyLink SCRM process that we will apply to the EIS contract. ***Figure 1.0-3*** is the CenturyLink process flow for disposal of government equipment.

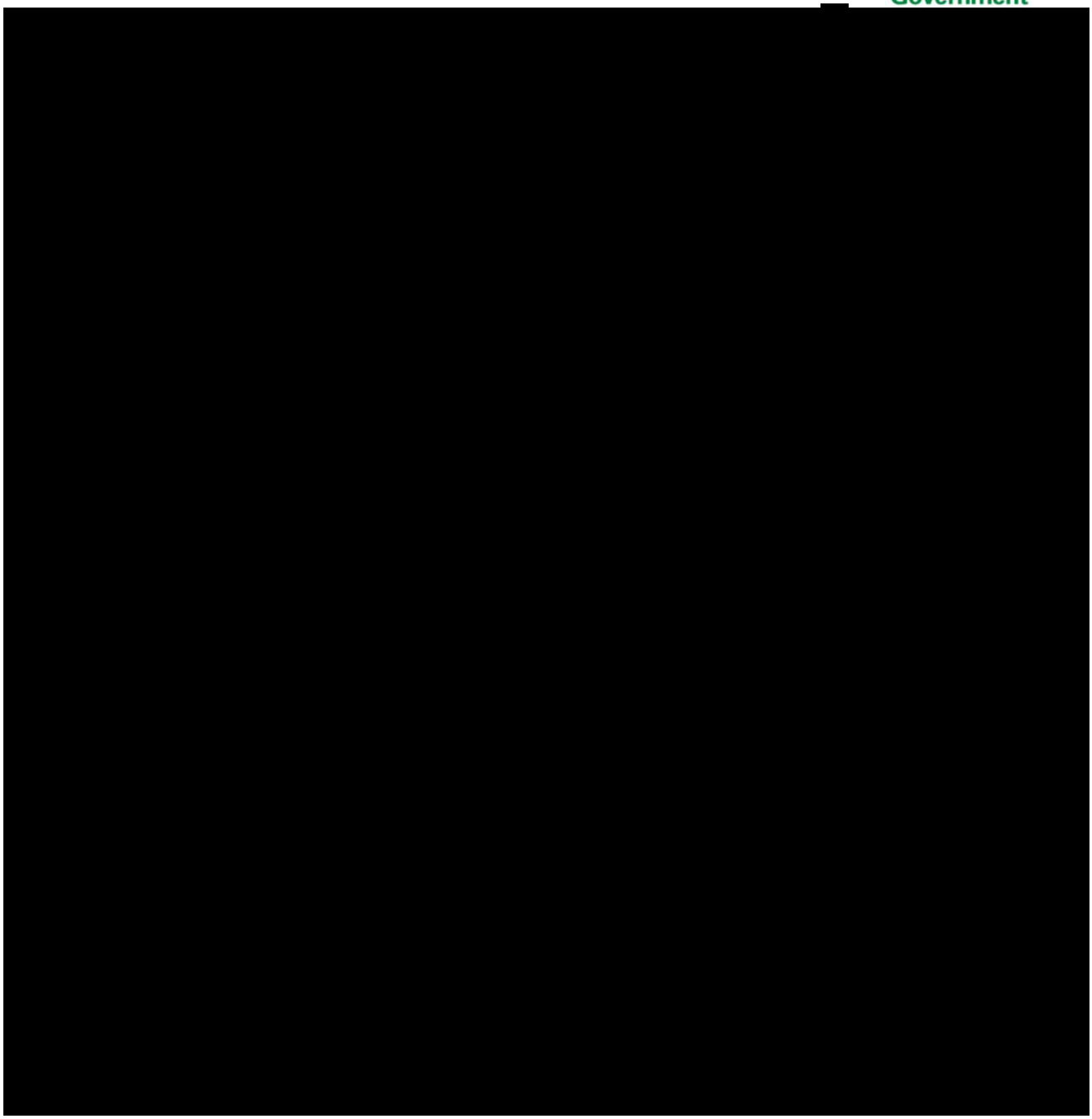

Figure 1.0-2. The CenturyLink Supply Chain Risk Management Process.

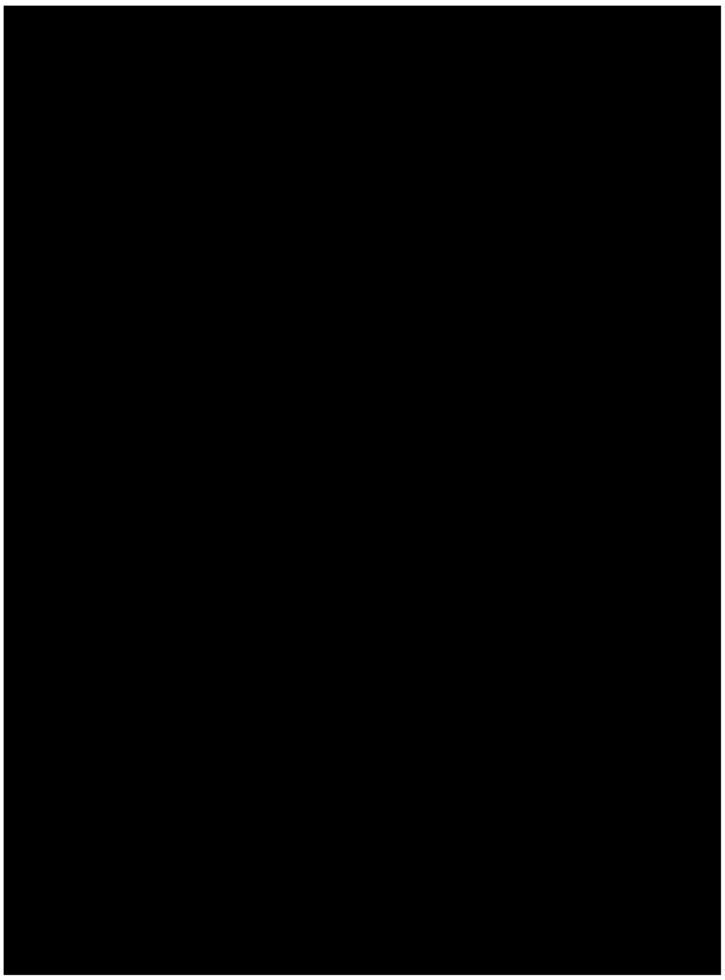

Figure 1.0-3. The CenturyLink Supply Chain Risk Management Process for Equipment Disposal

1.1 GENUINE INFORMATION TECHNOLOGY TOOLS (ITT) REQUIREMENTS

The CenturyLink SCRM process uses a set of genuine information technology tools (ITT) to ensure that the integrity of EIS hardware, software, and services is maintained. ***Figure 1.1-1*** summarizes the CenturyLink ITT that we will use for EIS and EIS TOs.

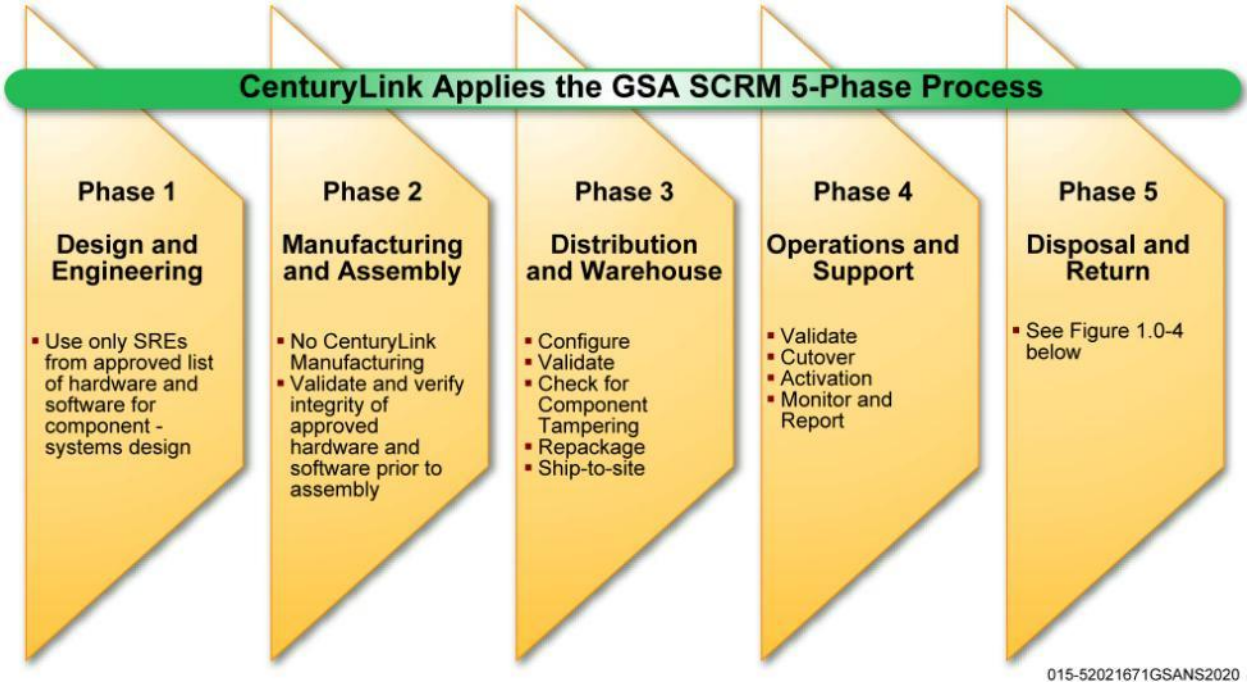

Figure 1.1-1: The CenturyLink Information Technology Tools (ITT). CenturyLink will use its established ITT for EIS and EIS Task Orders

The CenturyLink SCRM process begins with the design and procurement activities (Phase 1) to ensure that hardware and software resellers and OEMs provide only new, non-counterfeit, and unmodified equipment from certified and licensed OEMs and resellers. As discussed in Section 1.4-1, we ensure hardware and software are only purchased from sources that have been subject to our rigorous procurement processes.

The CenturyLink SCRM process is used at the CenturyLink warehouse (Phases 2 and 3). After the hardware and software are shipped to the CenturyLink warehouse, the warehouse conducts a high-level validation and verification of all received equipment. The process used by the CenturyLink warehouse to ensure equipment has not been tampered with during transit includes:

- **Receiving**
  - Visual (noninvasive) inspection
  - Random component testing (as required on a program-specific basis)
  - Documented and audited storage practices
    - Strict control over inventory by authorized personnel

- Separate parts/storage areas for different customers in secure areas
- No commingling of parts from different suppliers unless parts are sealed and easily identified

– General inventory audits

- **Returns and Excess Inventory Procedures**
  - Supplier sent damaged, poor quality, or wrong part: The warehouse notifies CenturyLink procurement. The supplier provides procurement with a return material authorization (RMA) and equipment is returned
  - Failed or defective network equipment tracked in inventory is first returned from the field to the warehouse using an enterprise resource planning (ERP) system to generate a stock transfer order (STO) and ship the equipment. The CenturyLink RMA coordinator will contact the supplier to open an RMA and:
    - Determination of warranty status
    - The supplier will send a like for like replacement and the replacement shipment will contain the return label for shipping the defective asset back to supplier. Once the replacement arrives, it will undergo the same receipt procedures as new equipment. The RMA coordinator will generate an STO to ship the defective unit back to supplier
    - If warranty is fix and repair, the defective item will be returned to the supplier to repair or replacement
  - Working equipment no longer needed in the field but is still of use to the program will be returned to warehouse using STO and placed in spare stock for that program
- **Excess Equipment**
  - Property management will send an inventory report to the government's property administrator requesting disposition instructions
    - When instructed, disposed equipment is sent to CenturyLink's reclamation group to scrap and salvage
  - For large dispositions, property management operates as above, provides an inventory report, and awaits government disposition instructions

- **Inventory Management**—this includes database input and reporting for:
  - Lifecycle asset management system
  - Work order delivery system for preventive maintenance
- **Staging and Installation**—we maintain equipment movement documentation and traceability by recording bar code data as the equipment moves through the warehouse and is tracked through installation (Phase 4)
- **Maintenance**—we maintain spare parts control and equipment movement documentation and traceability using the same bar code system and process
- **Disposal**—based on government disposition instructions (Phase 5)

Phase 4 the CenturyLink SCRM process is completed after the equipment is received at the government site. The equipment is again bar coded and the system is updated with the new location and status data. The CenturyLink installation technician will inspect the received equipment to ensure that the equipment has not been tampered with during reroute to the government site.

During phase 4 the CenturyLink SCRM process is conducted by the CenturyLink networks and security operations centers (NOC/SOC). Prior to cutover and activation the CenturyLink NOC/SOC does a final verification test to validate inventory integrity of the equipment.

1.2 System Security Engineering Process

Along with its SCRM process, CenturyLink will use engineering processes consistent with the NIST SP 800 161 IT requirements for EIS technical solution design and specification development. This process will include:

- Developing information security supply chain requirements in collaboration with the EIS PMO, GSA, and the TO agency
- Developing and applying detailed descriptions of SCRM practices and mitigation strategies
- Designing and developing test procedures
- Designing and developing independent verification and validation (IV&V) processes that support SCRM discovery and mitigation

1.3 IMPLEMENTING SCRM SECURITY REQUIREMENTS

To ensure that integrity and availability controls are in place for service related equipment (SRE), CenturyLink's supply chain management group monitors and distributes information on all known malicious content risks (e.g., unintentional supplier actions that allow potential unwanted functionality; auditing OEM and supplier security and manufacture processes). The CenturyLink supply chain management group will audit the supply chain risk processes and ensure they are all in line with current NIST and task order-specific requirements. The supply chain management group will work with CenturyLink design engineers to ensure that designs for EIS customers are in full compliance with current federal standards and the operational environments.

CenturyLink will apply security controls for the life of the EIS contract and tailor those controls to the specific TO. We will address the applicable controls we will use at the TO level.

1.4 CRITICALITY ANALYSIS (CA) PROCESS

CenturyLink procures products in support of all government requirements exclusively from OEMs and OEM-approved suppliers. CenturyLink considers all hardware and software (including associated components) as products supporting government information and communications technology (ICT). CenturyLink will only purchase new equipment from a licensed, approved OEM reseller or distributor.

For EIS, CenturyLink will require all federal direct suppliers to provide written SCRM plans covering their sold, installed, and maintained products. Every federal CenturyLink reseller, licensing, or distribution agreement addresses the requirement for such a plan. CenturyLink's federal procurement organization will identify and analyze all potential supplier and resupplier product sources for EIS. This analysis process includes:

- Focus on OEMs and resellers
- Execution of a checklist for supplier best practices
- Canvassing government and commercial sources regarding the suppliers products and determining other sources representational product assurance

Once initial analysis of an OEM or supplier suitability is completed, CenturyLink will conduct a more detailed evaluation of the supplier to make a final determination and document findings. To verify systems integrity, CenturyLink, as an acquirer of system level components, will request, as required for direct federal purchases, that potential EIS suppliers provide a detailed critical analysis at the architecture and sub-system level. Among the information that CenturyLink will request a supplier to provide are:

- Potential impacts to its product based upon system and subsystem threats
- A decomposition architecture that is aligned with potential threats
- Consideration of SCRM impacts that may be caused by potential threats
- Supplier testing and threat mitigation plan
- Representations and Certifications providing the supplier's corporate information including ownership and partnership entities
- Evaluation of supplier protection techniques such as plant and personnel security, packaging and shipping processes and component integrity checks

1.5 PRODUCT INTEGRITY

As shown in Section 1.1 above, CenturyLink uses a defined process to ensure that equipment resellers and OEMs only provide new (not repurposed), non-counterfeit, and unmodified hardware from certified and licensed OEMs and resellers. We ensure that all firmware and software is purchased only from government and CenturyLink-approved sources that are subject to our rigorous procurement processes. We include in our contractual terms and conditions with suppliers that equipment must be new (not refurbished).

We will continuously monitor the supply chain throughout a product's life cycle, including maintenance and repair. CenturyLink uses an ERP system to document the process, which is a government-approved material management system (OEM and supplier certifications are maintained by CenturyLink procurement on file). Using our ERP system, we will track purchased equipment, including spare parts, as follows:

- **Shipping to the CenturyLink warehouse**—The supplier will provide the OEM tracking numbers and electronic notice of shipment to CenturyLink and include this information in the packing list.
- **CenturyLink's warehouse and staging and receiving facility with floor-to-ceiling fencing; access-controlled and closed-circuit, TV-monitored to protect against unauthorized access; warehouse personnel hold a minimum of Secret clearances**—The CenturyLink warehouse technician will pull the packing list, inspect the package for signs of tampering and overall condition, affix a barcode on each item's package or directly apply it to the SRE. The technician then writes the barcode number and manufacturer's serial number on the packing list, and records the item in the ERP system. This system will capture project codes, part numbers, charge code, manufacturer, nomenclature, serial number, acquisition date, acquisition cost, equipment status, location, and asset identity (ID), at a minimum.
- **Shipping to a government site**—The ERP system generates requests to ship assets from the warehouse as an STO. When an SRE request is generated, the available warehouse inventory will be displayed and the requestor can select the items to be shipped. After the item is selected for shipment, an STO will be created as a PDF file and emailed to the CenturyLink warehouse, government property management, and the end destination. (Note: when an SRE is shipped from the CenturyLink warehouse or a supplier to a government location destination, we will ensure that CenturyLink installation personnel will be on site to receive the shipment.)
- **Site installation**—The CenturyLink installation technician will inspect the shipped package and SRE for signs of tampering and either scan for existing barcodes to validate a match with items shipped from our warehouse or affix a barcode and validate asset information contained on the purchase order if the item was shipped directly from a supplier.
  - Internal shipment: The installation technician will receive the shipment by logging into the ERP system and selecting the "Receive Shipment" option to update the system with the new location.

- Shipped directly from the supplier: The installation technician will mirror the warehouse receiving process and annotate the packing list and return the signed and dated purchase order with the barcode or serial number to CenturyLink property management.
- Integrity check: Once the SRE is installed, the site installation technician will run a full test profile, and prior to activation the NOC will conduct SRE operational integrity testing.

- **Preventive maintenance**—Preventive maintenance records will be tracked through CenturyLink's web-based work order delivery system, which includes the pre-defined maintenance schedule recommended by the OEM for the part number. Any location with a part onsite will receive an automated work order for preventive maintenance at the designated intervals. The work order delivery system is linked to the asset management system to identify all the locations for a particular part. The technician performing maintenance (or other sustainment activities) has limited access to the equipment and CenturyLink secure websites containing equipment configuration data. The technician must have pre-coordinated authorization to access the facility and then must log into the equipment using proper login information. This technician will log back into the work order delivery system once the work is complete and close the work order. The work order system maintains a history of all maintenance transactions.
- **Emergency maintenance**—For non-preventive maintenance calls, a trouble ticket will be generated from the NOC, which will dispatch a technician to the site to troubleshoot the problem. If defective equipment is found, the technician will request a replacement SRE to be dispatched from our warehouse to the site. A spare SRE will be shipped either from a supplier's or CenturyLink's warehouse to a repair activity. If shipped from the warehouse, a barcode will be affixed; if shipped from the supplier, the barcode will be affixed onsite. The defective part will be replaced and shipped to CenturyLink's warehouse for return to the supplier. The replacement part will be scanned and recorded in the ERP system. To verify integrity, prior to activation of a replacement SRE, components or

software, the NOC will run a full security scan and validation test on all replacement components.

  - ***Integrity Check***—Prior to activation of a replacement SRE, components or software, the NOC will run a full security scan and validation test on all replacement components.

- **De-installation and disposal**—When directed, the CenturyLink NOC will clean the SRE, and our site technician will de-install the SRE and ship the SRE back to the CenturyLink warehouse. The program office will inform property management if the equipment is no longer of use. The property management team will coordinate with the PMO and then prepare an SRE inventory for disposition as directed by the government. Prior to disposal, the warehouse will verify that SREs are fully sanitized and that all security-sensitive components and software are removed. Once an item is sent off for disposal, we retire those assets in the ERP system and maintain a historical file. See ***Figure 1.0-4*** for a representation of our disposal process.

1.6 SUPPLIER RELATIONSHIPS

As stated in Section 1.4, CenturyLink will apply our government-approved procurement system for purchase of federal EIS hardware and software. This system requires that we will only purchase EIS hardware and software from government authorized OEMs and resellers. CenturyLink has well established relationships with the primary OEMs we use for government and commercial programs. CenturyLink will not establish relationships with unknown or unidentified sources.

1.7 WARRANTY

CenturyLink warrants that the software supporting EIS is free from potential intrusion from items such as computer viruses, worms, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information.

CenturyLink will apply OEM warranties to all EIS commercial off-the-shelf (COTS) components consistent with Federal Acquisition Regulation (FAR) 52.246-17. In the event that the manufacturer's commercial warranty exceeds a period of one year, CenturyLink will pass this additional warranty period on to the government.

1.8 INDEPENDENT VERIFICATION AND VALIDATION

CenturyLink conducts security audits by a team that reports to our Chief Security Officer. This team will periodically perform reviews of its processes and systems to identify and remediate any weaknesses or vulnerabilities to internal CenturyLink EIS support activities. In addition to internal CenturyLink audits, the audit team will perform periodic audits on our federal OEMs and resellers, and their hardware and software providers to determine if these OEMs and resellers are complying with the EIS SCRM flow-down requirements including personnel, components (hardware and software), and services that are used to support EIS.

The audit team will conduct independent third party audits for verification and validation of the EIS supply chain's effectiveness in detection and prevention of counterfeit and illegally modified equipment known risks and evaluate the detection of new risk potentials and prevention capabilities of our SCRM process. CenturyLink will update annually its SCRM plan to include changes to the NIST SCRM guidelines Modifications to the SCRMP will be made at no cost to the government.

1.9 SUBCONTRACTOR RELATIONSHIPS

CenturyLink will incorporate the substance of RFP Section G.6.3 in subcontracts at all tiers where a subcontractor provides personnel, components, or processes identified as 1) a critical component, or 2) part of the CenturyLink supporting infrastructure which is required for delivery of a critical component. While NIST SP 800-161, Appendix F, defines broadly "critical component" as "a system element that, if compromised, damaged, or failed, could cause a mission or business failure," CenturyLink will look for direction, at the task order level, by government agency regarding the identification of a critical component within the services ordered. Upon such direction, CenturyLink will identify all of its subcontractors that will provide such critical components and ensure that these subcontractors provide CenturyLink all necessary information for CenturyLink

to complete and update annually its SCRM plan. All future changes to the SCRM plan will be in compliance with NIST SP 800-161.