Table of Contents (Continued)

List of Figures

3.0 SUPPLY CHAIN RISK MANAGEMENT PLAN [L.30.2.2, M.2.2, F.2.1 (77), G.6.3]

Lumen is pleased to include the EIS Supply Chain Risk Management (SCRM) Plan for MTIPS.

3.1 Purpose [L.30.2.2, G.6.3]

Lumen will implement a supply chain risk management methodology, described in this section, which is designed to meet the Government's requirements for the EIS MTIPS Services. This section describes Lumen's plan to manage supply chain risk throughout each of the five supply chain phases. Lumen's EIS MTIPS SCRM Plan policies and procedures will be based on supply chain risk management best practices using National Institute for Science and Technology (NIST) Special Publications 800-161 and 800-53 Revision 4 (including SA-12). In addition, to using the Government's NIST SCRM publications as a guide for the foundation to our EIS-MTIPS SCRM Plan, Lumen will utilize NIST's 10 Supply Chain Risk Management Practices, shown in **Figure 3.1-1.**

Figure 3.1-1. NIST's Ten (10) Supply Chain Risk Management Practices

NIST's 10 SUPPLY CHAIN RISK MANAGEMENT PRACTICES	
1) Uniquely identify supply chain elements, processes and actors	6) Use defensive design for systems, elements and process
2) Limit access and exposure within the supply chain	7) Perform continuous integrator review
3) Establish and maintain the provenance of elements, processes, tools and data	8) Strengthen delivery mechanisms
4) Share information within strict limits	9) Assure sustainment activities and processes
5) Perform supply chain risk management awareness and training	10) Manage disposal and final disposition activities throughout the system or element life cycle

Lumen is dedicated in supporting GSA's objective to ensure that an adversary will not sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. In addition, Lumen is committed to addressing GSA's intent to mitigate the threat of counterfeit and illegally modified products, and the enforcement of strict quality

control across the supply chain environment. Lumen will update the SCRM Plan to include any future changes to NIST SP 800-161 or other NIST Supply Chain Risk Management guideline(s). Any modification to the EIS MTIPS SCRM Plan will be made at no cost to the government.

3.2 Organizational Support

This document outlines Lumen's policies, processes and controls and will be focused on meeting GSA's SCRM requirements for Section C, as outlined in the EIS RFP (Sections: G, H, L). Lumen understands the importance of implementing risk management processes that address counterfeit and illegally modified products. Our risk management policies and processes will provide the framework for Lumen personnel to mandate, support and enforce appropriate measures in the mitigation of supply chain vulnerabilities. [redacted] As NIST guidelines, recommendations and standards evolve, Lumen will continue to update the EIS-MTIPS SCRM Plan annually and when significant changes occur.

3.2.1 Organizational Framework and Participation

Lumen's executive team is committed to ensuring that potential supply chain threats are closely monitored to minimize any negative impact to GSA's daily EIS mission and both short- and long-term EIS objectives. [redacted]

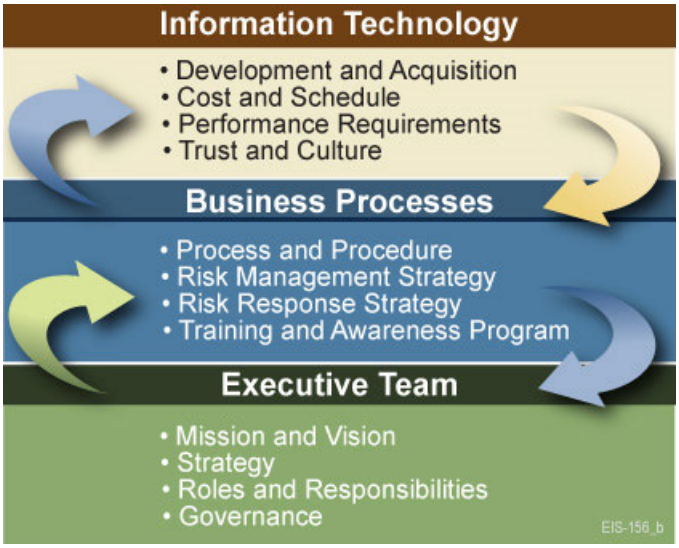


Figure 3.2.1-1. Risk Management Organizational Participation.

- ***The Executive Team*** establishes the appropriate structure and strategy for managing supply chain risk. The executive team has a keen understanding of the inherent risks involved in supplying EIS services. It is of critical importance to be vigilant as a service provider in identifying, managing, and mitigating supply chain risks to GSA for the EIS. The enforcement of strict quality control by Lumen of the applicable EIS OEM suppliers, resellers, and system integrators is the basis of the EIS-MTIPS SCRM Plan. The foundation of the plan is to mitigate the risk of counterfeit and illegally modified products within the EIS MTIPS infrastructure. In developing a Lumen EIS MTIPS-SCRM mission and vision statement, the executive team is focused on protecting the Lumen EIS infrastructure and customer information from physical and logical threats by stating:

Executive Team Mission

"Our mission is to ensure the security integrity of Lumen's EIS services from adversaries who look to sabotage Lumen EIS service infrastructure and/or customer information through surveillance, denial or disruption of service either physically or logically."

Executive Vision

"To protect the physical and logical security of the Lumen EIS Services."

- ***The Business Processes*** consist of the following tasks to be carried out by key functional areas within the Lumen organization for the EIS MTIPS-SCRM Plan: the development, implementation and execution of a risk management strategy, the assessment of risks and areas of vulnerabilities across the supply chain, the management and mitigation of risks across the five supply chain phases, the enforcement of quality control across suppliers via flow-down measures to ensure that MTIPS services are provided with genuine-non-counterfeit parts, products and components, the development and implementation of a training and awareness program across the Lumen organization to ensure an organization-wide understanding of the importance of and compliance with procedures set in place in the EIS MTIPS–SCRM Plan, to ensure the risk management strategy is adhered to.
- ***The Information Technology*** involves the Lumen EIS MTIPS service infrastructure, and equipment and software contained within the MTIPS security boundary. Numerous functional areas within Lumen may be included in the review of supply chain management risk but are not limited to: Product Management, Contracts and Legal, Network Architecture and Development, Backbone Engineering, Global Procurement and Corporate Security.

3.2.2 Organizational Support Model [L.30.2.2 (1), G.6.3 (1)]

To ensure that supply chain risks are effectively assessed, managed, documented, tracked, and controlled, Lumen recognizes that key stakeholders from various functional areas within the organization may be involved in overseeing supply chain risk management. This group of stakeholders will make up the Lumen EIS-MTIPS SCRM Control Board. The EIS-MTIPS SCRM Plan will be implemented by numerous subject matter experts (SME) from various Lumen key functional organizations that

comprise the EIS-MTIPS SCRM Control Board, at least the SMEs shown in **Figure 3.2.2-1.** Lumen recognizes the need for key functional areas to be engaged in ensuring risk levels are minimized and the integrity in the supply chain remains intact.

Figure 3.2.2-1. Lumen's SCRM Organizational Support Model.

3.2.2.1 Roles and Responsibilities

Procurement, Vendor Management, Corporate Security, Security Architecture Engineering Legal, Program Management Office (PMO), Network Operations, and Training. Other internal groups may also be involved during various milestones within the supply chain lifecycle.

Lumen has created a preliminary responsibility assignment matrix (RASCI matrix) shown in **Figure 3.2.2.1-1** as a starting point to help identify the roles and responsibilities for Lumen organizations that comprise the EIS-MTIPS SCRM Control Board. It is the expectation that additional controls and tasks will be added as risks are assessed and examined.

Figure 3.2.2.1-1. Preliminary Responsibility Assignment Matrix (RASCI) EIS-MTIPS SCRM Framework.

The RASCI will serve as a sample blueprint for an organizational-wide support structure for the EIS-MTIPS SCRM Plan and associated EIS-MTIPS SCRM Control Board. By identifying risk management controls and associated functional areas, Lumen believes the implementation of an EIS-MTIPS SCRM Plan can be successfully executed. It is well understood that each task order may carry with it a set of unique threats and security risks that will need to be managed on a customized basis. Lumen will ensure the foundational model for the EIS-MTIPS SCRM Plan is nimble enough to

not only support GSA's over-arching contract vehicle, but be able to be tailored to the unique characteristics of each task order. Lumen recognizes that both the controls and areas of responsibility may vary on a task-order to task-order basis. Therefore, Lumen acknowledges that there will need to be a rigorous, yet flexible approach to the implementation of the EIS-MTIPS SCRM Plan over the life of the IDIQ contract.

3.2.2.2 Supply Chain Risk Management Approach

[redacted]

Figure 3.2.2.2-1. Lumen's EIS-MTIPS SCRM Risk Identification Approach.

[redacted]

3.2.2.3 Supply Chain Risk Management Processes

[redacted]

Figure 3.2.2.3-1. Lumen's Five-Step Risk Management Process.

3.2.2.4 Supply Chain Risk Notification and Analysis

Figure 3.2.2-4-1. EIS-MTIPS SCRM Plan Risk Notification Process.

3.2.2.5 Policy Directives and Guidelines Followed

Supply chain risk management and analysis activities for the MTIPS service use the following guidelines as a reference as deemed appropriate:

- NIST 800-161, June 2014, **Supply Chain Risk Management Practices for Federal Information Systems and Organizations**
- NIST SP 800-30, September 2012 - Risk Management Guide for Information Technology Systems
- NIST SP 800-53 Revision 4, April 2013 and Latest Publication - Security and Privacy Controls for Federal Information Systems and Organizations (i.e., SA-12 controls)
- Federal Information Processing Standards (FIPS) Publication 199/200, February 2004 and March 2006
- DoD Instruction 5200.39, July 2008 - Critical Program Information (CPI) Protection within the Department of Defense
- DoD Instruction 5200.44, November 2012 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- National Institute of Standards and Technology Internal Reports (NISTIR) 7622, October 2012 - Notional Supply Chain Risk Management Practices for Federal Information Systems

3.2.2.6 Supply Chain Risk Management Plan Change Control

[redacted]

Figure 3.8.2.2.6-1. Task Order Based SCRM.

[redacted]

3.3 Supplier Management and Quality Control

[redacted]

Figure 3.3-1. Supplier Selection and Approval Process.

Lumen understands the challenges involved with acquiring new or replacement parts, components and software. It is of utmost importance to Lumen that the EIS-MTIPS SCRM Plan ensures that purchases made for services, software, hardware and components have already been examined and passed through a valid risk assessment process. Lumen requires that resellers, OEMs or systems integrators have furnished Lumen with their own SCRM Plan for our internal reviews and that all suppliers adhere to policies and laws ensuring that genuine parts and non–counterfeit components have been furnished to Lumen and/ or our customers.

3.3.1 Baseline Requirements for the EIS-MTIPS SCRM Plan

The following items will be addressed at minimum within the Lumen EIS-MTIPS SCRM Plan for EIS MTIPS services requiring initial control baselines per NIST Special

Publication 800 – 53 Revision 4 or the latest publication. Lumen's quality control measures are carried out in each of the five supply chain phases. Each phase of the supply chain requires a focus on supply chain risk assessment and mitigation efforts. Lumen'scontract vehicle that will be used to acquire products and services for the EIS MTIPS service will flow down Genuine ITT requirements to direct suppliers:

a. Lumen will perform and implement the EIS-MTIPS SCRM Plan in a reasonable manner for ITT that is delivered and installed for the configuration ordered and expected for the MTIPS service.
b. Lumen will require in each MAA and MSSA, that all resellers and suppliers have valid licenses for OEM equipment and software.
c. Lumen will exercise in each MAA and MSSA strict quality control thereby ensuring that all suppliers agree not to furnish counterfeit or illegally modified components, mitigating the risk of illegal modifications to relevant OEM products.
d. Lumen will ensure in each MAA that all suppliers will be required under the MAA to provide traceability of assurance and evidence of genuineness to the licensed product and component OEMs.

3.3.2 System Security Engineering

Lumen will implement as part of the EIS-MTIPS SCRM Plan, system security engineering processes and procedures that address new and existing software, hardware and infrastructure components. The system security engineering processes that will be established will help to ensure the integrity of system design, deployment and maintenance. The process will outline the development for integrating internal and external software and testing procedures that will help protect Lumen from external threats. In addition, the key functional areas within the organization will define the acceptance test criteria that will align closely with the EIS-MTIPS SCRM guidelines to ensure risk is managed, controlled and mitigated prior to deeming system readiness. Lumen will ensure key functional support areas work in tandem to manage risks by

documenting potential threats, implementing risk mitigation steps, and holding suppliers accountable to their SCRM Plans. The key functional areas will collaborate in documenting risk assessments that may affect GSA and develop recommendations for mitigation, remediation, and plans of action.

3.3.3 Security Control Implementation [L.30.2.2 (3), G.6.3 (3)]

The EIS-MTIPS SCRM plan will address the security controls for SA-12 (at least) as described in the NIST Special Publication 800-53 Revision 4 (**Figure 3.3.3-1**). The manner in which these controls are administered will be tailored in scope to the effort and specific information available at the time. Lumen understands that individual task orders may vary from contract level requirements and may present unique circumstances and provisions that may require Lumen to modify the implementation of such controls for GSA.

Figure 3.3.3-1. EIS-Solution SCRM Plan SA-12 Supply Chain Protection.

SA-12 CONTROL NUMBER	SUPPLY CHAIN PROTECTION	WITHDRAWN	ASSURANCE
SA-12 (1)	Supply Chain Protection/Acquisition Strategies/Tools/Methods		X
SA-12 (2)	Supply Chain Protection/Supplier Reviews		X
SA-12 (3)	Supply Chain Protection/Trusted Shipping and Warehousing	X Incorporated into SA-12(1)	
SA-12 (4)	Supply Chain Protection/Diversity of Suppliers	X Incorporated into SA-12(13)	
SA-12 (5)	Supply Chain Protection/Limitation of Harm		X
SA-12 (6)	Supply Chain Protection/Minimizing Procurement Time	X Incorporated into SA-12(1)	
SA-12 (7)	Supply Chain Protection/Assessments Prior to Selection/Acceptance/Update		X
SA-12 (8)	Supply Chain Protection/Use of All-Source Intelligence		X
SA-12 (9)	Supply Chain Protection/Operations Security		X
SA-12 (10)	Supply Chain Protection/Validate as Genuine and Not Altered		X
SA-12 (11)	Supply Chain Protection/Penetration Testing/Analysis of Elements, Processes and Actors		X
SA-12 (12)	Supply Chain Protection/Inter-Organizational Agreements		X
SA-12 (13)	Supply Chain Protection/Critical Information System Components		X

SA-12 (14)	Supply Chain Protection/Identity and Traceability		X
SA-12 (15)	Supply Chain Protection/Processes to Address Weaknesses or Deficiencies		X

3.3.4 Criticality Analysis (CA) [L.30.2.2 (4), G.6.3 (4)]

Lumen's key functional organizations and EIS-MTIPS SCRM Control Board will lead a Criticality Analysis (CA) effort, per NIST Special Publication 800-53 Revision 4 (or the latest published revision), that will develop processes and procedures to identify Mission Critical Functions supporting the contract level and individual task orders as part of the EIS-MTIPS SCRM Plan. Mission Critical Functions will include, at a minimum, elements and components that comprise key infrastructure and systems that support the Lumen EIS services requiring initial control baselines per NIST Special Publication 800-53, Revision 4 or the latest publication. Protection measures will be set in place to ensure system protection and mission effectiveness in supporting GSA's objectives. Several of the key functional teams involved in the CA effort may include SMEs from Corporate Security, Security Architecture Engineering, IT Development, Corporate Security, Vendor Management, Procurement, Network Operations and Business Development, along with other departments.

The CA team provides oversight for Lumen's key suppliers for hardware and software components supporting the MTIPS services. The team's analysis will include proof of company ownership for key suppliers; to include their component manufacturers, precise locations of corporate offices involved in the supply chain and assurances from suppliers that system protection techniques (to include countermeasures and sub-countermeasures) are utilized on material and components supplied to Lumen. A close examination of each supplier's procedures will be conducted to determine quality control and safety of such material.

Lumen's CA efforts will be in place to minimize risk and to ensure GSA that the objectives outlined by GSA will not be impaired due to vulnerabilities in system design. The risk of sabotage or subversion of a system's mission critical functions or critical components will be rigorously protected and attacks will be thwarted.

3.3.5 Criticality Analysis (CA)Product and Component Quality Control [L.30.2.2 (5), G.6.3 (5)]

The Lumen Team will ensure that products and components are not repaired and shipped as new products and components provided to the government. Lumen will only work with OEMs that exercise strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product and include traceability and evidence of genuineness of ITT back to the licensed product and component OEMs. Lumen will limit product acquisition activities to those OEMs and resellers that can ensure compliance with stated guidelines and agree to audits and assessments made by Lumen, the Government, or designated third parties, if deemed appropriate.

3.3.6 Criticality Analysis (CA)Supply Channel Monitoring [L.30.2.2 (6), G.6.3 (6)]

Lumen will ensure that all suppliers will be contractually obligated to furnish Lumen with documentation that ensures the authenticity and traceability of products which define the origination of such products and proof that they have not been subject to malicious intent during maintenance or repair. Quality control measures must be adhered to by suppliers of Lumen and suppliers will be contractually obligated to agree to audits and assessments made by Lumen, the Government or a designated third party at any time, if deemed appropriate. Lumen will validate components and products that are supplied as genuine – and will examine such components to ensure they have not been altered. Accurate packing slips, complete bill of materials, shipments being clearly marked and identified, packaging that follows the appropriate guidelines, examination of elemental damage to cartons, etc., will be reviewed and subject to inspection by Lumen to ensure the flow of genuine products.

3.3.7 Logical and Physical Delivery [L.30.2.2 (7), G.6.3 (7)]

Documented methods, procedures and guidelines for purchase orders and for the receiving department are critical to ensure the smooth flow of goods from suppliers to Lumen. Processes will be set in place to assist in the successful and safe receipt of

vendor equipment to the Lumen stocking warehouses. Strict shipment and packing standards, receiving processes, vendor return procedures, vendor audit processes, missing/incorrect paperwork, inconsistent packaging, software review and cycle count for spare inventory will be key elements included in the Lumen receiving procedures; which will be included as part of the EIS–MTIPS SCRM Plan for the MTIPS service. Physical access to warehouses and staging areas will be closely guarded and monitored. Electronic delivery of software will also be protected and will fall under the access control list methods and procedures for adequate supply chain protection.

Lumen will also evaluate the applicable suppliers' logistical methods and procedures to ensure that supply chain risk is avoided and well managed. For example, Lumen will evaluate all suppliers' ability to oversee material goods and services during the timeframe between the purchase order issuance and the actual delivery timeframe in order to limit opportunities for adversaries to corrupt information system components or products.

Guidelines prescribed by Lumen to the supply chain for MTIPS services will include, but will not be limited to, the following:

- Lumen suppliers will be instructed to deliver or transfer elements to a designated authorized recipient.
- Lumen will require suppliers to provide documentation of any nondestructive techniques or mechanisms to ensure that there is no unauthorized access throughout the delivery process.
- Lumen will require suppliers to utilize difficult-to-forge marks (such as digital signatures, hologram and/or nano tags) for all critical elements, which will be checked upon delivery and unpacking by authorized Lumen personnel.
- Lumen will require suppliers to utilize anti-tamper mechanisms for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g., tamper tape or seals).

- Lumen will require suppliers to document and monitor the logical delivery of elements, requiring downloading from approved, verification-enhanced sites.
- Lumen will require suppliers to obtain chain-of-custody for all critical hardware and require tamper-evident packaging.

Specific processes will be put in place that include step-by-step instructions to ensure strict quality control and access on a per purchase order basis. Protection mechanisms will look for evidence of:

- Packing slip is incorrect or not received with shipment
- Packing does not meet Lumen standards of receiving
- Shipments are not clearly identified
- Visible freight damage
- Incorrect quantities were shipped

All packages arriving in any Lumen stocking warehouse will be inspected for the following:

- Visible damages to outside cartons
- Secured pallets
- Elemental damage to cartons
- Inconsistent packaging

Processes will be set in place to ensure protection against the exposure of system components, information misuse, and unauthorized modification or redirection. Restricted access to warehouses and staging areas will ensure protection of system products and components. The reporting and documentation of supply chain issues that arise follow the following guidelines:

1. The PO Receiving Log will be used to keep track of deliveries and discrepancies unless otherwise directed by Lumen Logistics Management. For all issues below, it is assumed that the issue has been entered onto the Issue Log.

2. Lumen logistics team will be notified of new issues posted and addressed within assigned SLA.
3. All open issues will be reviewed regularly by the Lumen Logistics Management team.
4. Open issues exceeding any SLA will be escalated for resolution.
5. Any parts held in the stocking area will have a printed copy of the issue attached to it and are clearly marked for tracking and follow-up.

3.3.8 Operational Process [L.30.2.2 (8), G.6.3 (8)]

Lumen recognizes that it is of critical importance to ensure processes are in place to protect products and components during maintenance, patching, element replacement and other sustainment activities. Only authorized and documented personnel will have the ability to access elements of the MTIPS environment and Lumen-provided GSA equipment to repair and make changes to such gear, material and components. Guidelines and standards for repair, patching and maintenance will be followed by assigned personnel to ensure tasks are carried out in a manner consistent with protecting the Lumen supply chain and GSA. Configuration management tools and patch guidelines will be followed in strict accordance with processes set forth by Lumen. All steps performed with patching and maintenance will be entered in a maintenance log, to be audited by Lumen internal operations organizations as deemed appropriate. Disposal activities will follow a strict guideline to minimize unauthorized access to hardware, software and components. Careful labeling, tagging, tracking of goods that arrive and are disposed of by Lumen will be documented closely to ensure the protection of the supply chain for all items that arrive and leave Lumen. Disposal procedures must be followed carefully to maintain the integrity of the network. Personnel will be trained on proper disposal methods and procedures, the consideration of permanent disposal of elements will be reviewed and authorized disposers as needed will be properly vetted to ensure the safeguarding of elements and data during the disposal effort.

3.3.9 Supplier Relationship [L.30.2.2 (9), G.6.3 (9)]

A Lumen EIS Supplier Security Standard will be developed to ensure the selection of 1) OEMs, 2) Authorized resellers, or 3) Authorized partners/distributors. Lumen will not purchase from unknown/unidentified sources for the MTIPS services. All suppliers will be carefully selected and monitored throughout the supply chain life-cycle. All suppliers will be required to comply with the security standard set forth by Lumen and will be required to agree to be subject to audits and assessments by Lumen personnel. Clearly defined roles of each supplier will be identified. Procurements will follow the established Lumen Global Procurement Policy with each type of supplier and will be successful and approved only when Lumen can validate compliance to the Lumen best practices. Methods and procedures will be expected to be clearly identified by each supplier, as to limit counterfeit and illegally modified products from entering a suppliers' supply chain. Internal and external audits are expected to be conducted on a regular basis. Supplier reviews will be conducted to ensure:

- Counterfeit and illegally modified product training has been conducted and procedures are in place to ensure genuine products are supplied to Lumen.
- Suppliers provide transparency into their methods and procedures on how they ensure a secure supply chain environment.
- Verification of systems design and security processes have been furnished to Lumen
- Efficient and minimal delivery points of transit for goods and services is in place to limit supply chain vulnerabilities and access to system components.
- Provide proof that flow-down SCRM Plans are in place for the suppliers' lower-tier subcontractors which protects all materials, elements, products and components and delivery.

3.3.10 Software Warranty [L.30.2.2 (10), G.6.3 (10)]

Lumen will represent and warrant that (i) Lumen will not knowingly introduce Malicious Code into the Services, and (ii) throughout the term, Lumen will have in place

commercially reasonable measures to avoid the intrusion or insertion of any malicious code into the Service. For purposes of this Section, "malicious code" means viruses, worms, time bombs, Trojan horses, other harmful or malicious code, files, scripts, agents or programs or other malicious computer instructions or devices that materially erase data or programming, or materially infect, disrupt, damage, disable, or shut down a computer system or any material component of such computer system.

3.3.11 Verification and Validation [L.30.2.2 (11), G.6.3 (11)]

Lumen will reserve the right to perform security compliance assessments and audits of supplier facilities, networks, environments or systems. In the event of a security incident, Lumen may perform immediate audits of the affected facilities, networks and/or environments, as deemed appropriate for all suppliers. A periodic or continuous monitoring of supplier processes (determined on a case-by-case basis) will ensure that various Lumen key functional areas have transparency into the security control environment of each of the suppliers and suppliers' lower-tier subcontractors. In addition to assessments and verification activities, validation of such security requirements will be well documented.

3.3.12 Sub-Contractor Clause [L.30.2.2]

Lumen will incorporate the substance of EIS RFP Section G.6.3 in subcontracts at all tiers where an EIS subcontractor provides personnel, components, or processes identified as 1) critical components, or 2) part of the contractor's supporting infrastructure for the MTIPS service. All subcontractors providing applicable critical components or services will be identified and required to provide all necessary information to Lumen in order to complete the EIS-MTIPS SCRM Plan.

3.3.13 Training and Awareness

Lumen's Training Organization will support the development and delivery of EIS-MTIPS SCRM Plan training and awareness programs within Lumen. The training organization will develop and distribute a toolkit in an effort to introduce Lumen employees to the basic terms and concepts of the technology supply chain and

associated threats. In addition, the training will help to classify and familiarize the various supply chain participants, the OEMs, authorized resellers, integrators, etc., and advise associated suppliers of the associated risks that could be involved in the supply chain lifecycle. Employees and associated suppliers will be required on an as-needed basis to participate in supply chain training programs and assessments run by their own organizations; respectively.

3.4 Plan Submittal and Review [G.6.3.1]

Lumen understands that the EIS-MTIPS SCRM Plan is being submitted with the Lumen contract proposal in response to the EIS Request for Proposal. Updates will be submitted on an annual basis to the CO and COR, and when significant changes occur. All information as it is understood, will be treated as Controlled Unclassified Information pursuant to Executive Order 13556, shared only with Government agencies, and used solely for the purposes of mission essential risk management. It is understood that all reviews will be completed within a 45-day time period.

3.5 Definitions and Acknowledgements

3.5.1 Definitions

a) Lumen understands that “Information Technology” (see 40 U.S.C. 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

1. For the purpose of this definition, Lumen understands that equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires:
   a. Its use or;
   b. To a significant extent, its use in the performance of a service or furnishing of a product.

2. Lumen understands that the term “information technology’ includes computers, ancillary equipment (including imaging, peripherals , input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.
3. Lumen understands the term “information technology” does not include any equipment acquired by a contractor incidental to a contract.

Lumen understands that “Supply Chain Risk,” means that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

a. Lumen will maintain controls in the provision of applicable supplies and services to the Government to minimize supply chain risk.
b. Lumen recognizes that in order to manage supply chain risk, the Government may use the authorities provided in section 806 of Pub L. 111-383. Lumen understands that the Government may consider information, public and non-public, including all –source intelligence, relating to a contractor’s supply chain.
c. Lumen acknowledges that if the Government exercises the authority provided in section 806 Pub. L. 111.383 to limit disclosure of information, that no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

d. Lumen includes the substance of this clause, including this paragraph (e) in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

4.0 DRAFT BSS VERIFICATION TEST PLAN [L.30.2.3, M.2.2, E.2.1, F.2.1 (34-35), G.2.3, J.2]

Purpose

The purpose of the verification and acceptance testing is to ensure that Lumen's BSS meets all requirements specified in the EIS RFP Sections G and Sections J.2. This draft plan describes how we will support BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements and Section G.5.5.1 BSS Testing. Lumen will complete and pass the BSS validation testing, as stated in the contract, within 12 months from the acceptance of the BSS Verification Test Plan (see Section E.2.1).

4.1 Introduction and Overview

Lumen's EIS draft Business Support Systems (BSS) Verification Test Plan presented in this document is intended as a means to ensure that our BSS meets all of the performance and security requirements under the EIS contract.

BSS Verification Test Highlights

- More than 8 years of proven experience working with GSA to verify our operational and business support systems
- Extensive knowledge and experience with the GSA ATO process
- Ready to begin BSS verification process immediately upon EIS Notice to Proceed

Before initiating BSS verification testing outlined in this plan, the Lumen will provide written notice to the Government that we have internally validated that our BSS, as upgraded for EIS support, passed all unit testing and regression testing prior to interfacing with the GSA's system. Our internal testing will focus on ensuring that functional, regression, load, and security requirements have been met. All management and operations functions supporting Ordering, Billing, Inventory Management, Disputes, service level agreement (SLA) Management, and Trouble Ticketing processes will also be tested.

After EIS Notice To Proceed (NTP), we will incorporate any feedback on our draft BSS Verification Test Plan and provide a final plan within 30 days for review and approval by GSA. Within 21 days from the date of receipt of the final plan, the Government will accept or reject the plan. If it is rejected, Lumen will be given 14 days

to update the plan based on Government comments. Once we are authorized by GSA to commence the verification test process, noted in **Figure 4.1-1**, our testing will address all Test Scenarios and Test Cases outlined in this plan. The testing will use one or more test data sets provided by GSA and demonstrate how we meet the specified BSS acceptance criteria through the test results and analysis provided in a BSS Verification Test Results Report.

Figure 4.1-1. Lumen's BSS Verification Test Process. *Ensures GSA and EIS customer Agencies will be supported by quality systems.*

4.1.1 System Description

Lumen will develop our EIS BSS and supporting Web-based portal (the Lumen GSA Customer Portal) by expanding the capabilities of our current systems that are successfully supporting the Networx Enterprise and WITS 3 programs today. These systems provide an integrated approach to supporting all functions as specified in the GSA's EIS RFP for service ordering, billing, customer support, service management, inventory management and program management. By using Lumen's GSA Customer Portal, GSA and EIS customer Agencies can dramatically shorten administrative

workload times, thus obtaining internal cost savings due to increased efficiencies, with greater customer satisfaction and increased business results.

The GSA Customer Portal is installed on a secure server which is operated and maintained at [redacted] This provides the Government with redundant BSS capable of meeting Lumen's business continuity plan and supporting the EIS National Security and Emergency Preparedness requirements addressed in Section 1.1.1.10.4 of the management volume of this contract.

Figure 4.1.1-1 depicts the components within the Lumen GSA Customer Portal to be tested.

Figure 4.1.1-1. Lumen's GSA Customer Portal Architecture. *Provides GSA and EIS customer Agencies with a compliant and comprehensive approach to EIS BSS requirements.*

4.1.2 Test Organization

Figure 4.1.2-1 shows our test organization that is responsible for managing, coordinating, and conducting this test plan.

Figure 4.1.2-1. Test Organization Roles and Responsibilities.

ROLE	RESPONSIBILITY
Test Manager	• Coordinates all test activities and administrative tasks pertaining to the review • Ensures that the review is conducted in an orderly manner • Prepares and submits test reports
Test Lead	• Documents findings such as defects, inconsistencies, omissions, and ambiguities • Reports decisions and recommendations made by the test team • Logs and tracks issues in the Lumen case tool • Works with the Development Leads on resolutions and reporting daily status of the testing efforts
Test Team	• The test team is formed from the users of the system including: o GSA and agency representatives o CPMO Program Manager o CPMO Users and specified Lumen testers • The test team is responsible for: o Attending test sessions o Running test scripts o Formulating recommendations or corrective actions to assure defects, inconsistencies, omissions, and ambiguities are resolved quickly by the development teams

4.1.3 Test Environment

The Lumen Testing Organization will create a separate testing environment in Broomfield, CO enabling GSA or agency users to participate in testing. Creation of a testing laboratory consisting of required software, hardware and connection to the Lumen GSA Customer Portal will be provided.

4.1.4 Assumptions

- The following test conditions apply:
  - No testing between Lumen and GSA will occur until both systems have passed internal unit testing
  - All testing will be performed on the actual system to be used in delivering service (i.e., special purpose “test systems” will be used)
  - All data transfers will use the mechanism specified in Section J.2 for that data set
- Lumen will use GSA provided test data for all BSS verification testing unless specified otherwise:
  - This data will be used for testing purposes only
  - No customer “live” data will be used for testing

- This data will be a realistic simulation of actual customer data
- The test data will include, in some tests, intentional errors intended to test the Lumen's BSS error handling

- BSS testing will follow a tiered approach:
  - Lumen will accept multiple Test Cases for the Test Scenarios defined in Section E.2.1.2 of the RFP
  - Lumen will successfully execute each Test Case with one or more test data sets
  - GSA will group Test Data Sets into Test Subcases:
    - Each Test Subcase will contain data sets intended to test a specific "real world" Test Case (e.g., a complete and accurate disconnect order)
    - Each test subcase will include at least two complete Test Data Sets
- BSS functional testing acceptance:
  - Lumen's BSS will not have completed functional testing until all BSS Test Scenarios (Section 4 of this Plan) have passed and in accordance with Section H.21, Lumen may only accept and process task orders or service orders, provision or deliver services and bill for services after we receive written notification (1) from the CO that it has passed BSS testing and (2) from GSA that it has successfully completed security testing in accordance with G.5.6.
  - A Test Scenario is considered passed when the Lumen's BSS properly handles each associated Test Case
  - A Test Case is considered passed when the Lumen's BSS properly handles each associated subcase twice in succession using different data sets
  - A subcase is considered passed when Lumen's BSS properly handles the data sets following the prescribed actions with no errors or warnings

4.2 Scope [L.30.2.3, E.2.1.1]

Lumen will perform BSS verification testing in accordance with our GSA-approved BSS Verification Test Plan at a mutually acceptable date with the Government. Lumen will coordinate with GSA to allow Government representatives to observe all or any part of the verification testing. The scope of required BSS testing conducted with this plan includes:

- Verification that all BSS functional, regression, load, and security requirements have been successfully met
- Testing for all management and operation functions supporting Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes that are described in Sections G.3—G.8 and Section J.2
- Security testing based on functional requirements described in Section G.5.6 BSS Security Requirements. The security requirements acceptance will be based on Assessment and Authorization (A&A) and FedRAMP certification, if applicable
- Execution of multiple Test Scenarios and Test Cases (see Section 4.0 of this Plan)
- Execution of Test Cases for quality, utility and customer access features

In addition, after we successfully pass the initial acceptance testing described in this plan, we will perform retests as requested by the Government to ensure continued compliance each time a new service is offered, or we modify features and/or functionality of the BSS that affect the functional requirements described in Sections G. If the Government requests this retest, Lumen will provide a BSS Verification Test Results report, including analysis, within 7 days after performance of the tests. This testing will continue until the results are acceptable to the Government.

4.3 Methodology and Approach to Verification Test scenarios and test cases [E.2.1.5.1]

Lumen's BSS Test Strategy is designed to ensure that all Test Scenarios and Test Cases defined by GSA are thoroughly exercised to ensure all appropriate combinations of test situations are covered. In addition, all RFP references are mapped against the Test Scenarios to ensure that the original intent of each requirement is accurately captured.

In order to streamline the process and to facilitate evaluation, we will develop test scripts to organize the testing in the most logical sequence possible, with pre-defined data input, expected output, and defined testing iterations and phases. Test data input and output will be carefully identified to clearly indicate the associated test packages involved in specific testing tasks.

The process is also designed to flow in a logical manner, which simulates actual real-world work scenarios. Order establishment is followed by typical MACD (move, addition, change and delete) scenarios to exercise system capabilities. Billing and inventory output is also provided at the appropriate points in the process. Using this method, every order flow, billing, and inventory scenario is represented by appropriate testing. BSS security and functionality testing is supported as detailed in Section 4.13 of this Plan as well as account management, including setup and role-based access.

4.4 Test Scenarios and Test Cases [L.30.2.3 (4), E.2.1.2, E.2.1.3, G.3 - G.5, G.7, J.2]

The Government has defined 13 Test Scenarios and 38 Test Cases that must pass acceptance testing. All Test Scenarios and Test Cases described in this section must pass within 12 months from the date of issuance of the NTP, or else the contract will be canceled. **Figure 4.4-1** contains a high-level list of BSS Test Scenarios for which the BSS must pass the defined acceptance criteria. Each Test Scenario is associated with one or more Test Cases defined in the subsections that follow. Lumen will address the specific functional requirements defined in the relevant portions of the EIS RFP Sections G and J in the Test Scripts we develop for each test scenario. The Test Scripts

will also address all relevant data exchange mechanisms and the validation of data exchanged. Lumen will support BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements.

Figure 4.4-1. BSS Test Scenarios

TEST SCENARIO #	RFP REFERENCES	DESCRIPTION	ACCEPTANCE CRITERIA
BSS-TS01	• E.2.1.3.1 • G.5.3.2 • J.2.9	Exchange structured data using the defined direct data exchange methods: • XML via secure web services • Pipe, "|", delimited table via Secure File Transfer Protocol (SFTP)	Lumen will demonstrate bidirectional exchange of defined data structure that meets the interface specifications as defined in Section G.5.3.2 and Section J.2.9.
BSS-TS02	• E.2.1.3.2 • G.3 • J.2.3	Lumen's BSS manages the following as specified in Section J.2.3: • Provide Direct Billed Agency Setup	Lumen will demonstrate successful TO Data Management initial setup and updates.
BSS-TS03	• E.2.1.3.3 • G.5 • J.2.3	Lumen's BSS manages role-based access control to all BSS functions (e.g., ordering, billing, inventory management, trouble management, SLA management)	Lumen will demonstrate that its BSS provides the ability to define role-based users with privileged access to the BSS to meet the requirements as defined in Section J.2.3.
BSS-TS04	• E.2.1.3.4 • G.3 • G.5.3.1 • J.2.4	Lumen's BSS manages the processing of orders and generation of required acknowledgments and notifications. Order types include: • New service for each of the services specified in Section C.2, Technical Requirements, that are included in the awardee's contract • Service Moves • Service Disconnects • Service Feature Changes • Telecommunications Service Priority (TSP) • Auto-sold CLINs • Bulk Orders	Lumen will demonstrate that an authorized Government user can place an order using the methods specified in Section J.2.4 and the order populates the fields in the Lumen BSS in a way that meets the requirements in Sections G.3, G.5 and J.2. Using the direct data exchange method defined in Section J.2.4, Lumen will demonstrate that our BSS can provide all required Contract Deliverables Requirements Lists (CDRLs) including: 1) Service Order Acknowledgement 2) Service Order Rejection Notice 3) Service Order Confirmation 4) Firm Order Commitment Notice 5) Service Order Completion Notice
BSS-TS05	• E.2.1.3.5 • G.3 • J.2.4 • J.2.10.1.1.4.3	Lumen's BSS handles order supplements/updates that impact other, in-progress orders: • Cancel orders • Service Feature Changes • Location changes	Lumen will demonstrate that an authorized Government user can place a change or cancel order using the methods specified in Section J.2.4 and the order populates the fields in the Lumen BSS in a way that meets the requirements in Sections G.3, G.5 and J.2.2. Using the direct data exchange method defined in

TEST SCENARIO #	RFP REFERENCES	DESCRIPTION	ACCEPTANCE CRITERIA
		• Changes to Customer Want Date • Changes to administrative data	Section J.2.4, Lumen will demonstrate that our BSS can provide all required CDRLs including: 1) Service Order Acknowledgement 2) Service Order Rejection Notice 3) Service Order Confirmation 4) Firm Order Commitment Notice 5) Service Order Completion Notice
BSS-TS06	• E.2.1.3.6 • G.3 • J.2.4	Lumen's BSS handles orders for administrative changes to the records for previously provisioned services as described in G.3	Lumen will demonstrate that an authorized Government user can place an administrative change order using the methods specified in Section J.2.4 and the order populates the fields in the Lumen BSS in a way that meets the requirements in Sections G.3, G.5 and J.2.2. Using the direct data exchange method defined in Section J.2.4, Lumen will demonstrate that our BSS can provide all required CDRLs including Service Order Administrative Change
BSS-TS07	• E.2.1.3.7 • G.3 • G.5.3 • J.2.4	Lumen's BSS manages Self-Service Provisioning and other Rapid Provisioning orders and provides the correct notices.	Lumen will successfully demonstrate the completion of these orders. Non-self-service orders will be tested using both correctly placed orders and orders with related errors. Self-service orders will be tested with correctly placed orders and to ensure that the Lumen BSS does not permit the placement of incorrect orders. Using the direct data exchange method defined in Section J.2.4, Lumen will demonstrate that our BSS can provide all required CDRLs including: 1) Service Order Acknowledgement 2) Service Order Completion Notice
BSS-TS08	• E.2.1.3.8 • G.3 • G.4 • G.7 • J.2.4 • J.2.5 • J.2.6 • J.2.7 • J.2.10	Lumen's BSS properly manages inventory and billing: • Generates the inventory of services delivered by Lumen • Produces output that is consistent with order and billing details • Generates the detailed billing in accordance with the Billing Invoice (BI) CDRL • Properly handles usage-based billing • Calculates billing based on Lumen's awarded pricing	Lumen will demonstrate that its service inventory management system maintains a complete and accurate inventory of EIS service orders in a way that meets the requirements in G.7 and G.5 and Section J.2 Contractor Data Interaction Plan (CDIP) and is verified and accepted by GSA. Lumen will demonstrate that the output of its billing data elements is consistent with the orders entered into our BSS and that the billing data elements meet the requirements in Sections G.3, G.5 and J.2.2. Using the direct data exchange method defined in Sections J.2.5-J.2.7, Lumen will demonstrate that its BSS can provide all required CDRLs including:

TEST SCENARIO #	RFP REFERENCES	DESCRIPTION	ACCEPTANCE CRITERIA
		• Correctly calculates the Associated Government Fee (AGF) due to GSA and produces the required AGF CDRLs • Provides accurate calculation of rounding and proration related to Billing, Taxes, Fees and Surcharges	1) Billing Invoice 2) Billing Adjustment 3) Tax Detail 4) AGF Detail 5) AGF Electronic Funds Transfer Report 6) Inventory Reconciliation
BSS-TS09	• E.2.1.3.9 • J.2.3 • J.2.6	Lumen's BSS properly manages all dispute types with appropriate handling for: • Billing disputes • Inventory disputes • SLA disputes • Dispute tracking and reporting	Lumen will demonstrate that our BSS can accept and issue disputes as well as tracking them to resolution. Using the direct data exchange method defined in Sections J.2.5-J.2.7, Lumen will demonstrate that our BSS can provide all required CDRLs including: 1) Dispute 2) Dispute Report
BSS-TS10	• E.2.1.3.10 • G.3 • J.2.4 • J.2.10.3	Lumen's BSS properly manages SLA Management: • SLA Reporting • SLA Credit Request handling and response	Lumen will demonstrate that our BSS successfully tracks SLAs with associated key performance indicators (KPIs) as well as reporting SLA performance and providing sufficient information to response to SLA Credit Requests. Using the direct data exchange method defined in Sections J.2.5-J.2.7, Lumen will demonstrate that our BSS can provide all required CDRLs including: 1) SLA Report 2) SLA Credit Request Response
BSS-TS11	• E.2.1.3.11 • G.4 • G.5 • J.2.10.2	Lumen's BSS produces acceptable open-format reports defined in the CDIP: • Monthly Billing Information Memorandum • Trouble Management Incident Performance Report • Trouble Management Performance Summary Report	Lumen will demonstrate, via sample reports, that the open-format reports specified are sufficiently detailed and clear so as to meet the Government's requirements.
BSS-TS12	• E.2.1.3.12 • G.5.5	Lumen's BSS testing includes regression testing of all key features including ordering, service assurance, and billing. NOTE: Applies only to testing conducted as part of system changes,	Lumen will demonstrate that our BSS meets regression testing. The final BSS test plan will include regression testing; however, actual regression testing will not be part of initial test and acceptance.

TEST SCENARIO #	RFP REFERENCES	DESCRIPTION	ACCEPTANCE CRITERIA
		not initial BSS development.	
BSS-TS13	• E.2.1.3.13 • G.5.6	Lumen's BSS has passed A&A as defined in Section G.5.6.	Lumen will demonstrate that our BSS meets FISMA Moderate requirements.

The individual Test Cases stipulated in EIS RFP Section E.2.1.3 are defined in the figures in subsections 4.4.1 through 4.4.13. Each Test Case figure includes the following headings:

- Test Scenario: The associated test scenario from **Figure 4.4-1** above
- Test Case ID: Identification number for the Test Case
- Test Case Description: Brief title of the Test Case
- Requirements Reference(s): Where the functional requirements that are being tested can be found in the EIS RFP
- Prerequisites: Actions that must be completed prior to implementing the Test Case (in addition to the general prerequisites for all testing defined in Section 1.4)
- Government Input(s): Data the Government will provide as input to the Test Case
- Expected BSS Output(s): Expected data or actions from Lumen's BSS
- Data Set Description: Brief description of the data sets the Government will provide as part of testing
- Acceptance Criteria: Factors to be checked prior to acceptance of the test results. **Figure 4.4-2** defines the terms used.

Figure 4.4-2. Acceptance Criteria Terms

CRITERIA	DEFINITION
Successful data transfer	Lumen demonstrates that data transmitted was received intact without error using the formats and mechanisms descr bed in the Test Case.
Correct technical aspects	Lumen demonstrates that data transfers were completed using the correct mechanism, in the correct format, and with the correct structure.

CRITERIA	DEFINITION
Evidence of failure notification	Lumen demonstrates that expected notifications of failure were properly issued.
No partial import	Lumen demonstrates that their BSS does not import partial data in cases where the data is corrupt or otherwise cannot be imported in full.
All required CDRLs	Lumen demonstrates that the expected CDRLs (listed in the expected output section) are all delivered.
Accurate data based on inputs	Lumen demonstrates that the data provided in CDRLs is accurate and reflects the data provided by the Government inputs and the prerequisites.
Access granted	Lumen demonstrates that the user gains access to resources as expected.
Access denied	Lumen demonstrates that the user is denied access to resources as expected.
No errors displayed	Lumen demonstrates that the user is not shown any unexpected errors.
Appropriate errors are displayed	Lumen demonstrates that the user is shown the expected errors.
CDRLs are internally consistent	Lumen demonstrates that the data provided in the expected CDRLs is internally consistent between the set of CDRLs.
Complies with calculation rules	Lumen demonstrates that the data provided in the CDRLs matches that which would be expected based on rounding and proration calculation requirements.
Each CDRL meets requirements	Lumen demonstrates that the provided CDRLs meet the requirements specified by the Government (used for CDRLs without detailed format requirements). Standard requirements include, at minimum: • CDRL contains the required information • CDRL is clear and readily understood
Lumen BSS receives ATO	Lumen demonstrates that the BSS has received Authorization to Operate (ATO) and has been approved by GSA based on relevant security requirements as defined in Section G.5.6 and references therein.

4.4.1 BSS-TS01: Direct Data Exchange

Figure 4.4.1-1. BSS-TS01-01: XML over Secure Web Services

TEST SCENARIO	BSS-TS01: DIRECT DATA EXCHANGE
TEST CASE ID	BSS-TS01-01
TEST CASE DESCRIPTION	XML OVER SECURE WEB SERVICES
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Properly formatted Government data set listed as using web services as the transfer mechanism in Section J.2
Expected Output(s)	• Properly formatted Lumen data set that meets the following criteria: o Listed as using web services as the transfer mechanism in Section J.2 o Includes data derived from the Government input

Acceptance Criteria	• Successful data transfer • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o One Government data set listed as using web services as the transfer mechanism in Section J.2

Figure 4.4.1-2. BSS-TS01-02: PSV over SFTP

TEST SCENARIO	BSS-TS01: DIRECT DATA EXCHANGE
TEST CASE ID	BSS-TS01-02
TEST CASE DESCRIPTION	PSV OVER SFTP
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Properly formatted Government data set listed as using SFTP as the transfer mechanism in Section J.2
Expected Output(s)	• Properly formatted Lumen data set that meets the following criteria: o Listed as using SFTP as the transfer mechanism in Section J.2 o Includes data derived from the Government input
Acceptance Criteria	• Successful transfer of PSV data • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o One Government data set listed as using SFTP as the transfer mechanism in Section J.2

Figure 4.4.1-3. BSS-TS01-03: Error Handling: XML over Secure Web Services

TEST SCENARIO	BSS-TS01: DIRECT DATA EXCHANGE
TEST CASE ID	BSS-TS01-03
TEST CASE DESCRIPTION	ERROR HANDLING: XML OVER SECURE WEB SERVICES
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Invalid Government data set listed as using web services as the transfer mechanism in Section J.2
Expected Output(s)	• Notification to Lumen of failed import
Acceptance Criteria	• Evidence of failure notification • No partial import
Data Set Description	• Each Government-provided test data set will include: o One Government data set listed as using web services as the transfer mechanism in Section J.2 o One or more XML formatting errors (e.g. missing delimiters)

Figure 4.4.1-4. BSS-TS01-04: Error Handling: PSV over SFTP

TEST SCENARIO	BSS-TS01: DIRECT DATA EXCHANGE
TEST CASE ID	BSS-TS01-04
TEST CASE DESCRIPTION	ERROR HANDLING: PSV OVER SFTP
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Invalid Government data set listed as using SFTP as the transfer mechanism in Section J.2
Expected Output(s)	• Notification to Lumen of failed import
Acceptance Criteria	• Evidence of failure notification • No partial import
Data Set Description	• Each Government-provided test data set will include: o One Government data set listed as using SFTP as the transfer mechanism in Section J.2 o One or more formatting errors (e.g., missing delimiters)

4.4.2 BSS-TS02: Task Order Data Management

Figure 4.4.2-1. BSS-TS02-01: Direct Billing Account Setup

TEST SCENARIO	BSS-TS02: TASK ORDER AND ACCOUNT MANAGEMENT SETUP
TEST CASE ID	BSS-TS02-01
TEST CASE DESCRIPTION	DIRECT BILLING ACCOUNT SETUP
Requirements Reference(s)	• G.3 • J.2.2 • J.2.3
Prerequisites	• N/A
Government Input(s)	• Task order controlled data as defined in Section J.2.3 • Task order associated data as defined in Section J.2.3 • System Reference data as defined in Section J.2.3
Expected Output(s)	• Direct Billed Agency Setup (DBAS) CDRL
Acceptance Criteria	• All required CDRLs as defined in Section J.2.3 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o Sample TO controlled data transferred in the form of a sample TO o Sample TO associated data transferred in free format (not previously defined) unless the Lumen specifies in their proposal that customer registration is to be submitted via their web interface and that interface collects all of the required data o Sample System Reference data transferred using the mechanism specified in Section J.2

4.4.3 BSS-TS03: Role Based Access Control

Figure 4.4.3-1. BSS-TS03-01: Authorized User Access Verification

TEST SCENARIO	BSS-TS03: ROLE BASED ACCESS CONTROL
TEST CASE ID	BSS-TS03-01
TEST CASE DESCRIPTION	AUTHORIZED USER ACCESS VERIFICATION
Requirements Reference(s)	• G.5 • J.2.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• User attempts to: o Sign into BSS o Access BSS areas to which they are an authorized user o Exercise the full range of functionality (read/write) permitted for their role
Expected Output(s)	• User is permitted to: o Access to BSS o Access BSS areas as authorized o Exercise assigned functionality
Acceptance Criteria	• Access is granted • No security errors displayed
Data Set Description	• Each Government-provided test data set will include: o Role to be tested o Functionality to be tested

Figure 4.4.3-2. BSS-TS03-02: Unauthorized User Access Denial Verification

TEST SCENARIO	BSS-TS03: ROLE BASED ACCESS CONTROL
TEST CASE ID	BSS-TS03-02
TEST CASE DESCRIPTION	UNAUTHORIZED USER ACCESS DENIAL VERIFICATION
Requirements Reference(s)	• G.5 • J.2.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• User attempts to: o Sign into BSS o Access BSS areas to which they are not an authorized user o Exercise functionality (read/write) not permitted for their role

TEST SCENARIO	BSS-TS03: ROLE BASED ACCESS CONTROL
TEST CASE ID	BSS-TS03-02
TEST CASE DESCRIPTION	UNAUTHORIZED USER ACCESS DENIAL VERIFICATION
Expected Output(s)	• User is denied access at the point appropriate the role, area and functionality specified in the test data set: o Access to BSS o Access to specific BSS areas o Access to specific functionality o User is shown security error message
Acceptance Criteria	• Access is denied • Appropriate errors are displayed
Data Set Description	• Each Government-provided test data set will include: o Role to be tested (may be specified as none if the set is intended to show denial of unauthorized users) o Functionality to be tested

4.4.4 BSS-TS04: Service Ordering

Figure 4.4.4-1. BSS-TS04-01: New Order via Web Interface

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-01
TEST CASE DESCRIPTION	NEW ORDER VIA WEB INTERFACE
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.10.2.1.15
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o SO to be entered into Lumen's BSS via the Lumen's web interface as described in Section G.5.3.1

Figure 4.4.4-2. BSS-TS04-02: New Order via Email

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-02
TEST CASE DESCRIPTION	NEW ORDER VIA EMAIL
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.10.2.1.15
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o SO submitted via a means listed in J.2.4 other than the Lumen's web interface

Figure 4.4.4-3. BSS-TS04-03: Disconnect Order

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-03
TEST CASE DESCRIPTION	DISCONNECT ORDER
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • Previously provisioned circuit or service element entered into the Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for the disconnect of • A circuit or service element (CLIN) • A feature of a circuit or service element

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-03
TEST CASE DESCRIPTION	DISCONNECT ORDER
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) if required based on the requirements described in Section J.2.4 o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for the disconnect of a circuit or service element or a feature of a circuit or service element as described in Section G.3 and Section J.2.10.1.1.4.2

Figure 4.4.4-4. BSS-TS04-04: Feature Addition Order

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-04
TEST CASE DESCRIPTION	FEATURE ADDITION ORDER
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • Previously provisioned circuit or service element entered into the Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for the addition of a feature to a circuit or service element
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for the addition of a feature to a circuit or service element as described in Section G.3 and Section J.2.10.1.1.4.2

Figure 4.4.4-5. BSS-TS04-05: Move Order

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-05
TEST CASE DESCRIPTION	MOVE ORDER
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • Previously provisioned circuit or service element entered into the Lumen BSS
Government Input(s)	• Two Service Orders (SOs) that combine to specify the move of a circuit or service element with all required data elements as described in Section J.2.4 • One SO for the disconnect of the circuit or service element at the old location • Second SO for the installation of the identical circuit or service element at the new location
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A pair of complete SOs for the move of a circuit or service element from one valid location to another as described in Section G.3 and Section J.2.10.1.1.4.2 o SO for the disconnect from the old location o SO for the installation of the identical service at the new location

Figure 4.4.4-6. BSS-TS04-06: TSP Order

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-06
TEST CASE DESCRIPTION	TSP ORDER
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) requesting TSP with all required data elements as descr bed in Section J.2.4

Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO with a TSP code for one or more services listed in Section C.2 of the contract

Figure 4.4.4-7. BSS-TS04-07: Auto-Sold CLINs

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-07
TEST CASE DESCRIPTION	AUTO-SOLD CLINS
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) that includes CLINS with associated Auto-Sold CLINs and contains all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO that includes Auto-Sold CLINs for one or more services listed in Section C.2 of the contract

Figure 4.4.4-8. BSS-TS04-08: Task Order Unique CLINs (TUC)

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-08
TEST CASE DESCRIPTION	TASK ORDER UNIQUE CLINS (TUCS)
Requirements Reference(s)	• G.3 • J.2.4

Prerequisites	• TO setup data loaded into Lumen BSS • TO Data defines one or more TUCs • Account Management data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) containing Task Order Unique CLINs (TUCs) and all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO containing Task Order Unique CLINs (TUCs) for one or more services listed in Section C.2 of the contract

Figure 4.4.4-9. BSS-TS04-10: Bulk Orders

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-10
TEST CASE DESCRIPTION	BULK ORDERS
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Bulk Service Order (SO) with all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Confirmation (SOC) o Firm Order Commitment Notice (FOCN) o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A SO including at least 20 line items for services listed in Section C.2 of the contract o SO data provided via a delimited text file or MS Excel file

Figure 4.4.4-10. BSS-TS04-11: Error Checking: Missing Info

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-11
TEST CASE DESCRIPTION	ERROR CHECKING: MISSING INFORMATION
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) missing one or more required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Rejection Notice (SORN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o SO missing one or more required data elements for one or more services listed in Section C.2 of the contract

Figure 4.4.4-11. BSS-TS04-12: Error Checking: Invalid Info

TEST SCENARIO	BSS-TS04: SERVICE ORDERING
TEST CASE ID	BSS-TS04-12
TEST CASE DESCRIPTION	ERROR CHECKING: INVALID INFO
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with one or more invalid data elements as descr bed in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Service Order Rejection Notice (SORN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o SO orders with one or more invalid data information for one or more services listed in Section C.2 of the contract o Invalid data can include improperly formatted data or data that is inconsistent with the TO or Account Management data

4.4.5 BSS-TS05: Supplements to In-Progress Orders

Figure 4.4.5-1. BSS-TS05-01: Cancel Orders

TEST SCENARIO	BSS-TS05: SUPPLEMENTS TO IN-PROGRESS ORDERS
TEST CASE ID	BSS-TS05-01
TEST CASE DESCRIPTION	CANCEL ORDERS
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as descr bed in Section J.2.4 • Service Order (SO) for a cancellation of the previous order with all required data elements as described in Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Updates to Service Order Confirmation (SOC) if required o Updates to Firm Order Commitment Notice (FOCN) if required o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o A second SO canceling the first Service Order as defined in Section J.2.10.1.1.4.3 o The Cancel Order may be issued before or after the deadline described in Section G.3

Figure 4.4.5-2. BSS-TS05-02: Service Feature Change

TEST SCENARIO	BSS-TS05: SUPPLEMENTS TO IN-PROGRESS ORDERS
TEST CASE ID	BSS-TS05-02
TEST CASE DESCRIPTION	SERVICE FEATURE CHANGE
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a service feature change to the previous order with all required data elements as described in Section J.2.4 issued prior to completion to previous order

Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Updates to Service Order Confirmation (SOC) if required o Updates to Firm Order Commitment Notice (FOCN) if required o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o A second SO descr bing a service feature change to the first Service Order as defined in Section J.2.10.1.1.4.3

Figure 4.4.5-3. BSS-TS05-03: Location Change

TEST SCENARIO	BSS-TS05: SUPPLEMENTS TO IN-PROGRESS ORDERS
TEST CASE ID	BSS-TS05-03
TEST CASE DESCRIPTION	LOCATION CHANGE
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as descr bed in Section J.2.4 • Service Order (SO) for a location change to the previous order with all required data elements as descr bed in Section J.2.4 issued prior to completion to previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Updates to Service Order Confirmation (SOC) if required o Updates to Firm Order Commitment Notice (FOCN) if required o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o A second SO describing a location change to the first Service Order as defined in Section J.2.10.1.1.4.3

Figure 4.4.5-4. BSS-TS05-04: Change to Customer Want Date

TEST SCENARIO	BSS-TS05: SUPPLEMENTS TO IN-PROGRESS ORDERS
TEST CASE ID	BSS-TS05-04
TEST CASE DESCRIPTION	CHANGE TO CUSTOMER WANT DATE
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a change to the Customer Want Date for the previous order with all required data elements as descr bed in Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Updates to Service Order Confirmation (SOC) if required o Updates to Firm Order Commitment Notice (FOCN) if required o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o A second SO descr bing a change to the Customer Want Date for the first Service Order as defined in Section J.2.10.1.1.4.3 o The Customer Want Date Change Order may be issued before or after the deadline described in Section G.3

Figure 4.4.5-5. BSS-TS05-05: Change to Administrative Data

TEST SCENARIO	BSS-TS05: SUPPLEMENTS TO IN-PROGRESS ORDERS
TEST CASE ID	BSS-TS05-05
TEST CASE DESCRIPTION	CHANGE TO ADMINISTRATIVE DATA
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a change to the administrative data for the previous order with all required data elements as described in Section J.2.4 issued prior to completion of the previous order

Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) o Updates to Service Order Confirmation (SOC) if required o Updates to Firm Order Commitment Notice (FOCN) if required o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services listed in Section C.2 of the contract o A second SO describing a change to the administrative data for the first Service Order as defined in Section J.2.10.1.1.4.3

4.4.6 BSS-TS06: Administrative Change Orders

Figure 4.4.6-1. BSS-TS06-01: Administrative Change Order

TEST SCENARIO	BSS-TS06: ADMINISTRATIVE CHANGE ORDER
TEST CASE ID	BSS-TS06-01
TEST CASE DESCRIPTION	ADMINISTRATIVE CHANGE ORDER
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders
Government Input(s)	• Administrative Change Order that specifies a change to the administrative data associated with a previously provisioned service as described in Section G.3
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Administrative Change (SOAC)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete administrative change order for a change to the administrative data for a previously provisioned service as descr bed in Section G.3

4.4.7 BSS-TS07: Rapid Provisioning & Self-Provisioning Orders

Figure 4.4.7-1. BSS-TS07-01: Rapid Provisioning Orders

TEST SCENARIO	BSS-TS07: RAPID PROVISIONING & SELF-PROVISIONING ORDERS
TEST CASE ID	BSS-TS07-01
TEST CASE DESCRIPTION	RAPID PROVISIONING ORDERS
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) for one or more services subject to rapid provisioning as defined in Section G.3 with all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours o Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o A complete SO for one or more services subject to rapid provisioning as defined in Section G.3

Figure 4.4.7-2. BSS-TS07-02: Self-Provisioning Orders

TEST SCENARIO	BSS-TS07: RAPID PROVISIONING & SELF-PROVISIONING ORDERS
TEST CASE ID	BSS-TS07-02
TEST CASE DESCRIPTION	SELF-PROVISIONING ORDERS
Requirements Reference(s)	• G.3 • G.5.3.2 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for one or more services that are: o Subject to rapid provisioning as defined in Section G.3 o Available for self-provisioning as defined in Section G.3 and Section C.2
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: o Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours o Service Order Completion Notification (SOCN)

TEST SCENARIO	BSS-TS07: RAPID PROVISIONING & SELF-PROVISIONING ORDERS
TEST CASE ID	BSS-TS07-02
TEST CASE DESCRIPTION	SELF-PROVISIONING ORDERS
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o Service Order (SO) with all required data elements as descr bed in Section J.2.4 for one or more services that are subject to rapid provisioning as defined in Section G.3 and that are available for self-provisioning as defined in Section G.3 and Section C.2

Figure 4.4.7-3. BSS-TS07-03: Self-Provisioning Orders: Error Checking

TEST SCENARIO	BSS-TS07: RAPID PROVISIONING & SELF-PROVISIONING ORDERS
TEST CASE ID	BSS-TS07-03
TEST CASE DESCRIPTION	SELF-PROVISIONING ORDERS: ERROR CHECKING
Requirements Reference(s)	• G.3 • G.5.3.2 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS
Government Input(s)	• Service Order (SO) for one or more services subject to rapid provisioning as defined in Section G.3 and available for self-provisioning • Populated via the Lumen Portal with one or more missing or invalid data elements as descr bed in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4 • Service Order Rejection Notice (SORN) • User is shown error message indicating failure
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects • Appropriate errors are displayed
Data Set Description	• Each Government-provided test data set will include: o Service Order (SO) with all required data elements as described in Section J.2.4 for one or more services that are subject to rapid provisioning as defined in Section G.3 and that are available for self-provisioning as defined in Section G.3 and Section C.2 o SO to be provided via the Lumen Portal

4.4.8 BSS-TS08: Inventory and Billing

Figure 4.4.8-1. BSS-TS08-01: Inventory Reconciliation

TEST SCENARIO	BSS-TS08: INVENTORY AND BILLING

TEST CASE ID	BSS-TS08-01
TEST CASE DESCRIPTION	INVENTORY RECONCILIATION
Requirements Reference(s)	• G.7 • J.2.7
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders
Government Input(s)	• N/A
Expected Output(s)	• Inventory Reconciliation (IR) CDRLs as descr bed in Section J.2.7
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• N/A, see Prerequisites

Figure 4.4.8-2. BSS-TS08-02: Billing

TEST SCENARIO	BSS-TS08: INVENTORY AND BILLING
TEST CASE ID	BSS-TS08-02
TEST CASE DESCRIPTION	BILLING
Requirements Reference(s)	• J.2.5 • J.2.10
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders
Government Input(s)	• N/A
Expected Output(s)	• Billing CDRLs as defined in Section J.2.4: • Billing Invoice (BI) • Tax Detail Report (TAX) • Associated Government Fee Detailed (AGFD) • AGF EFT Report (ATR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects • CDRLs are internally consistent • Complies with calculation rules
Data Set Description	• N/A, see Prerequisites

Figure 4.4.8-3. BSS-TS08-03: Usage Based Billing

TEST SCENARIO	BSS-TS08: INVENTORY AND BILLING
TEST CASE ID	BSS-TS08-03
TEST CASE DESCRIPTION	USAGE BASED BILLING
Requirements Reference(s)	• G.3 • J.2.4

TEST SCENARIO	BSS-TS08: INVENTORY AND BILLING
TEST CASE ID	BSS-TS08-03
TEST CASE DESCRIPTION	USAGE BASED BILLING
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously usage based provisioned orders
Government Input(s)	• Sample usage data for one or more UBI based on Usage Based CLIN(s)
Expected Output(s)	• Billing CDRLs as defined in Section J.2.4: o Billing Invoice (BI) o Tax Detail Report (TAX) o Associated Government Fee Detailed (AGFD) o AGF EFT Report (ATR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects • CDRLs are internally consistent • Complies with calculation rules
Data Set Description	• Each Government-provided test data set will include: o Sample usage data for one or more UBI based on Usage Based CLIN(s) o See also Prerequisites

Figure 4.4.8-4. BSS-TS08-04: Billing Adjustments

TEST SCENARIO	BSS-TS08: INVENTORY AND BILLING
TEST CASE ID	BSS-TS08-04
TEST CASE DESCRIPTION	BILLING ADJUSTMENTS
Requirements Reference(s)	• G.4 • J.2.5
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders • At least one previously submitted Billing Invoice (BI)
Government Input(s)	• Sample adjustment request to change or modify a billing line item
Expected Output(s)	• Billing Adjustment (BA) as defined in Section J.2.5: • Reflects requested adjustment
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each Government-provided test data set will include: o Sample adjustment request to change or modify a billing line item

4.4.9 BSS-TS09: Dispute Handling

Figure 4.4.9-1. BSS-TS09-01: Government Initiated Dispute

TEST SCENARIO	BSS-TS09: DISPUTE HANDLING
TEST CASE ID	BSS-TS09-01
TEST CASE DESCRIPTION	GOVERNMENT INITIATED DISPUTE
Requirements Reference(s)	• J.2.3 • J.2.6.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders • At least one previously submitted Billing Invoice (BI)
Government Input(s)	• Government issues at least 2 Disputes (D) as defined in Section J.2.6 • Notification to close a dispute after first Dispute Report is issued (see expected outputs)
Expected Output(s)	• Dispute Report (DR) • Reflects open Disputes • A second Dispute Report (DR) • Reflects open and closed Disputes
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects

Data Set Description	• Each Government-provided test data set will include:
	  ○ At least two Disputes (D)
	  ○ Notification to close one or more disputes

4.4.10 BSS-TS10: SLA Management

Figure 4.4.10-1. BSS-TS10-01: SLA Reporting

TEST SCENARIO	BSS-TS10: SLA MANAGEMENT
TEST CASE ID	BSS-TS10-01
TEST CASE DESCRIPTION	SLA REPORTING
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders
Government Input(s)	• Services to show as SLAs met or missed
Expected Output(s)	• SLA Report (SLAR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Services by UBI to show as SLAs met or missed

Figure 4.4.10-2. BSS-TS10-02: SLA Credit Request

TEST SCENARIO	BSS-TS10: SLA MANAGEMENT
TEST CASE ID	BSS-TS10-02
TEST CASE DESCRIPTION	SLA CREDIT REQUEST
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.3.1.19
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into Lumen BSS • One or more previously provisioned orders • At least one previously submitted Billing Invoice (BI) • SLA Report with at least one SLA missed
Government Input(s)	• SLA Credit Request (SLACR)
Expected Output(s)	• SLA Credit Request Response
Acceptance Criteria	• All required CDRLs • Each CDRL meets requirements
Data Set Description	• Each Government-provided test data set will include: o SLA Credit Request

4.4.11 BSS-TS11: Open-Format Reporting

Figure 4.4.11-1. BSS-TS11-01: Open-Format Reporting: Samples

TEST SCENARIO	BSS-TS11-01: OPEN-FORMAT REPORTING
TEST CASE ID	BSS-TS11-01
TEST CASE DESCRIPTION	OPEN-FORMAT REPORTING: SAMPLES
Requirements Reference(s)	• G.4 • G.5 • J.2.10.2.1.13 • J.2.10.2.1.25 • J.2.10.2.1.26
Prerequisites	• N/A
Government Input(s)	• N/A
Expected Output(s)	• Sample copies of the Lumen's standard reports for: o Monthly Billing Information Memorandum o Trouble Management Incident Performance Report o Describes service outage or degradation that are user initiated and/or automated monitoring created reports o Trouble Management Performance Summary Report
Acceptance Criteria	• Each CDRL meets requirements
Data Set Description	• N/A

4.4.12 BSS-TS12: Regression Testing

Figure 4.4.12-1. BSS-TS12-01: Regression Testing

TEST SCENARIO	BSS-TS12: REGRESSION TESTING
TEST CASE ID	BSS-TS12-01
TEST CASE DESCRIPTION	REGRESSION TESTING: TEST CASES TBD
Requirements Reference(s)	• G.5.5
Prerequisites	• Lumen BSS has completed Development testing and ATO
Note	• Inputs, outputs, acceptance criteria and datasets to be determined based on Change Management provided in G.5.5 • Additional Test Cases may be defined as needed

4.4.13 BSS-TS13: Security Testing [L.30.2.3 (3), G.5.6]

Lumen will develop our EIS BSS following all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. We will comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines, GSA IT security directives, policies and guides, and other appropriate Government-wide laws and regulations for protection and security of Government IT. Our development approach described in our BSS Risk Management Framework Plan will ensure the correct implementation of security controls, auditability, access controls, data protection, and backup and recovery of the BSS. A detailed description of our methods will be provided as part of the System Security Plan which will be delivered to the Government within 30 days of NTP, and updated throughout the contract period of performance as needed.

The correct implementation of the security controls specified in NIST Special Publication 800-53 Revision 4 for FIPS 199 Impact Level Moderate systems will be assessed as part of this Verification Test Plan, noted in **Figure 4.13-1** using the processes defined in NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems to achieve system ATO and FedRAMP compliance.

Figure 4.4.13-1. BSS-TS13-01: Security Testing

TEST SCENARIO	BSS-TS13: SECURITY TESTING
TEST CASE ID	BSS-TS13-01

TEST CASE DESCRIPTION	SECURITY TESTING
Requirements Reference(s)	• G.5.6
Prerequisites	• Defined in Section G.5.6 and references therein
Government Input(s)	• Defined in Section G.5.6 and references therein
Expected Output(s)	• Defined in Section G.5.6 and references therein
Acceptance Criteria	• Lumen BSS receives ATO
Data Set Description	• Defined in Section G.5.6 and references therein

4.5 Test Results [E.2.1.4]

The Lumen Team will demonstrate that it successfully meets the BSS acceptance criteria for the various test scenarios/test cases defined in Sections E.2.1.2 and E.2.1.3. Lumen will provide detailed test results from all Test Cases executed as part of this plan that provides evidence of successful testing as follows:

- Functional requirements for the Ordering, Billing, Inventory Management, Disputes, SLA Management and trouble ticketing processes as described in Section G and Section J.2
- System to system data exchange mechanism requirements defined in Section G.5 for each CDRLs defined in Section J.2
- Correct CDRLs are used in the data exchange
- Mandatory data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate
- Available optional data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate
- Timely and successful system to system data exchange to meet defined performance SLAs and provisioning intervals

The test results will detail at a minimum the following:

- Test scenario #
- Test case #
- Test Data Set #
- Test #

- Date of Test Performed
- Acceptance Criteria
- Test Result (Pass/Fail)

In addition, Lumen will include the following data as applicable:

- Attendance and Participation in the Test
- Names of Test manager, test lead and test team members
- Description of each defect found, by type, by class, and severity
- Disposition of the defect
- Disposition of the overall testing

4.6 Timeline and Test Sequencing [E.2.1.5.1]

Lumen will provide BSS verification testing as required in Section E of the EIS RFP and based on the following timeline and sequencing.

- Draft BSS Verification Test Plan submitted with proposal
- Final BSS Verification Test Plan submitted 30 days after NTP
- Final BSS Verification Test Plan accepted or rejected by Government within 21 days
- Revisions to BSS Verification Test Plan 14 days after receipt of Government comments
- Internal testing of the Lumen BSS
- Written notice to the Government of Lumen's BSS passing internal testing
- Testing of the cases in section 4.1 through 4.13 in support of the 13 test scenarios between the Lumen BSS and the Government BSS. An acceptable mutually agreed upon date for testing will be determined.
- Lumen will provide the Government with a BSS Verification Test Results Report that includes analysis of the current testing and a summary table of all previously submitted test results, within seven days after performance of the tests.
- The Government reserves 14 days to accept or reject the test results

4.7 Deliverables [E.2.1.5; F.2.1 (34-35)]

Lumen will provide a final BSS Verification Test Plan that is based on the test methodology described above within 30 days of NTP. We will not process any orders for EIS products and services prior to successfully completing all verification testing and acceptance by the Government. We will rerun the verification tests as required for accepted changes to CDRLs or data exchange mechanisms acceptance criteria during the life of the contract.

Upon completion of the initial BSS Verification Test and after any retest over the life of the contract, Lumen will provide the Government a detailed BSS Verification Test Results Report. This report will include analysis of the current testing performed and a summary table of all previously submitted test results. This report will be due within 7 days after performance of the tests. After delivery, the Government will have 14 days to accept or reject the test results, in part or in whole.

Lumen will perform a re-test of any Test Cases with test data sets that failed until they are accepted by the Government. We will also rerun tests, in part or in whole, as deemed necessary by the Government, to verify that the Government's comments on the test results are satisfactorily addressed. All deliverables for BSS Verification Testing are outlined in **Figure 4.7-1**.

Figure 4.7-1. BSS Verification Testing Deliverables

ID	REQUIREMENT REFERENCE	DELIVERABLE DESCRIPTION REFERENCE	DELIVERABLE NAME	FREQUENCY	DELIVER TO
34	E.2.1.5.1	E.2.1.5.1	BSS Verification Test Plan	Draft: with proposal Final 30 days after NTP Updates: within 14 days of Government request	GSA CO
35	E.2.1.5.2	E.2.1.5.2	BSS Verification Test Results Report	Initial: 7 days after test completion Update: As needed	GSA CO

4.8 References

Compliance references include:

- Federal Information Security Management Act (FISMA) of 2002, available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
- NIST Special Publication 800-18 Rev 1, "Guide for Developing Security Plans for Federal Information Systems."
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments."
- NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems."
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."

- NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems.”
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.”
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide.”
- NIST Special Publication 800-88 Revision 1, “Guidelines for Media Sanitization.”
- NIST Special Publication 800-128, “Guide for Security-Focused Configuration Management of Information Systems.”
- NIST Special Publication 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations.”

In addition to complying with the requirements identified in the Government policies, directives and guides specified above, Lumen will comply with the current GSA policies, directives and guides listed below:

- GSA Information Technology (IT) Security Policy, CIO P 2100.1(I).
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook”.
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior.”
- GSA Order CPO 1878.1, “GSA Privacy Act Program.”
- GSA IT Security Procedural Guide 01-01, “Identification and Authentication.”
- GSA IT Security Procedural Guide 01-02, “Incident Response.”
- GSA IT Security Procedural Guide 01-05, “Configuration Management.”
- GSA IT Security Procedural Guide 01-07, “Access Control.”
- GSA IT Security Procedural Guide 01-08, “Audit and Monitoring.”
- GSA IT Security Procedural Guide 04-26, “FISMA Implementation.”

- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program.”
- GSA IT Security Procedural Guide 06-29, “Contingency Plan Testing.”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”
- GSA IT Security Procedural Guide 06-32, “Media Protection Guide.”
- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide.”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan.”
- GSA IT Security Procedural Guide 08-43, “Key Management Guide.”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide.”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide.”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity.”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection.”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program.”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide.”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide.”
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing December 2011.
- The Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony,” April 2007.

5.0 EIS SERVICES VERIFICATION TEST PLAN [L.30.2.4, M.2.2, E.2.2, E.2.2.1, F.2.1 (36), C.2, G.8]

5.1 Purpose and Objective

Lumen's EIS Services Verification Test Plan presented in this document is intended as a means to ensure services ordered by customer agencies meet performance requirements stated in the EIS contract and, as required, subsequent Task Order (TO) award. The objective of the verification and acceptance tests is to ensure satisfactory end-to-end service performance and proper operation of all ordered features and functions. Performance will be considered satisfactory when services, equipment, systems and their associated features and functions perform as specified in the contract and TO.

5.2 EIS Test Plan Change Control

Upon GSA approval, this plan constitutes Version 3.0 of the EIS Services Verification Test Plan. Changes to this document occur under the following scenarios, with all changes subject to GSA and awarding agency review and approval:

Addition of New Services. As Lumen's service offerings under the EIS contract evolve during the life of the contract, additional test cases will be submitted for all new services added to the contract with the contract modification.

Task-Order Specific Testing. An agency may define additional testing in the TO. Lumen will submit additional test cases based on these requirements, and conduct associated testing upon TO award.

Changes to Existing Services. As regulations, standards, technologies, and services evolve, Lumen will update tests outlined in this document to ensure currency and compliance to new requirements.

5.3 Verification And Acceptance Testing Approach [E.2.2.5]

Lumen will comply with all requirements in Section E.2.2.5 of the solicitation. Lumen provides verification and acceptance testing of all awarded EIS Services as described in Figure 5.3-1. Upon TO award, Lumen completes verification and acceptance testing

based on the acceptance criteria defined in the Government accepted EIS Test Plan. GSA and/or agency representatives have the option to observe these tests, and agencies may conduct acceptance testing subsequent to the verification testing conducted. Agencies may conduct additional acceptance testing subsequent to the verification testing conducted by Lumen. Our Acceptance Testing includes Government compliance requirements such as FedRAMP for cloud services, and the Authority to Operate (ATO) for FISMA related security requirements for EIS services. The Lumen Team will not begin billing for services if the government rejects the services within three (3) days of receipt of the SOCN. Lumen will issue a new SOCN for services after correcting the reasons for rejection.

Figure 5.3-1. Lumen's EIS Services Verification and Testing Process.

If the government exercises any of the options listed in Section E.2.2.5 and identified in Figure 5.3-1 as a consequence of unacceptable acceptance testing results, all expenses incurred by the government will be borne by Lumen. If before circuit acceptance the government elects option 1, the Lumen Team will immediately initiate corrective actions to remedy the problem reported on the trouble ticket and shall keep

the government informed of progress. In cases when the government cannot successfully complete acceptance testing due to circumstances beyond the control of the Lumen Team, we will notify government of the details surrounding the deficiencies and the steps we have taken to overcome the deficiencies. On a case-by-case basis, the GSA CO or the OCO may choose to waive the acceptance testing or extend the testing period. If the waiver is not granted, the Lumen Team will be obligated to continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

Lumen provides all necessary test equipment required to conduct tests listed in this document, including data terminals, load boxes, test cables, and any other hardware and software required for testing. As shown in the figure above, the effective billing date for an EIS Service starts upon agency approval of acceptance testing procedures and EIS Testing Report. Lumen will conduct additional tests as required by the awarding agency to confirm proper operation of a delivered EIS service defined by the TO.

5.4 EIS Service Verification Tests

Lumen's EIS Test Plans and Procedures detail the standard test procedures utilized to verify that services delivered under the EIS program meets the performance specifications defined in the EIS RFP. Lumen is responsible for the verification testing of the EIS services, and Government is responsible for reviewing and approving the recorded acceptance tests which Lumen will provide the Government within 3 days of service installation and testing.

For each service order, Lumen will verify that the services delivered to the Government meet the requirements of the specific service order. GSA also has the option of observing or having a representative observe all or any part of the verification testing.

Sections 5.4.1, 5.4.2 and 5.4.3 provide details of our EIS Service Verification Tests.

5.4.1 Test Scenario TS-01 [C.2]

Objective	Demonstrate that the proposed Cloud Service is compliant with Federal Risk and Authorization

	Management Program (FedRAMP) requirements as defined.
Approach	The IaaS, PaaS, and SaaS infrastructures have been granted a Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board (JAB) at a Moderate impact level based upon the Federal Information Processing Standards (FIPS) 199 classification. Following a rigorous security review, the JAB approved a P-ATO that an executive department or agency can leverage to issue a security authorization and an accompanying ATO. This allows U.S. federal, state, and local Governments to more rapidly realize the benefits of the cloud. Government agencies can also request the platform specific FedRAMP security package at any time. FedRAMP also provides for continuous compliance monitoring. Once granted a P-ATO, CSPs are monitored and assessed annually and must demonstrate their service offerings remain in compliance.
Acceptance Criteria	FedRAMP certification is verified and accepted by GSA.

5.4.1.1 Approach to Compliance

FedRAMP has replaced FISMA authorizations as the preferred approach to validating the security of cloud services and requires cloud providers to receive an independent security assessment, conducted by a third-party assessment organization (3PAO), to sell cloud services to a federal agency. This assessment is conducted on an annual basis in order for the CSP to remain FedRAMP approved.

FedRAMP also provides for continuous compliance monitoring. Once granted a P-ATO, CSPs are monitored and assessed annually and must demonstrate their service offerings remain in compliance.

5.4.1.2 Status of Compliance

IaaS, PaaS and SaaS platforms are all FedRAMP compliant. The Lumen Team solution for PaaS and SaaS is provided through Microsoft, which is FedRAMP compliant as noted with ***Figure 5.4.1.2-1***. The Lumen Team solution for IaaS is provided through several Teammates. IaaS provided through Day1 has secured a P-ATO as noted in ***Figure 5.4.1.2-2***. IaaS solution provided through Amazon Web Service (AWS) has the FedRAMP PackageID of AGENCYAMAZONGC. IaaS solution provided by Teammate GDIT has a FedRAMP PackageID of F1303191948. The Lumen Team can provide FedRAMP package information if required during performance of the contract to security personnel as requested.

FedRAMP
Federal Risk Authorization Management Program

September 9, 2015

Re: Microsoft Significant Change for Global Foundation Services and Windows Azure

Mr. Zander,

This letter is to inform you of the successful inclusion of Microsoft's significant change request to include your government-specific offerings within your FedRAMP Joint Authorization Board Provisional Authorization.

Specifically:

- **Microsoft Global Foundation Services (GFS)**: This authorization now includes the GFS Government Services Offering (GSGO).
- **Windows Azure Public Cloud Solution:** This authorization now includes the Microsoft Azure Government Offering.

If you or any of your customers have any questions about this, please do not hesitate to put them in touch with me.

Thanks.

Matt Goodrich, JD
FedRAMP Director, GSA
matt.goodrich@gsa.gov | 202.870.6231

cc:
Gabi Gustaf
Susie Adams

Figure 5.4.1.2-1. Lumen's Teammate's PaaS and SaaS FedRAMP Certificate

December 14, 2015

Mr. Stephen R. Kovac
Vice President, Colocation and Cloud Services
Day1 Solutions, Inc.
1751 Pinnacle Drive, Suite 425
McLean, VA 22102

Mr. Kovac,

The Joint Authorization Board (JAB) of the Federal Risk and Authorization Management Program (FedRAMP) has completed the security review of the Day1 Solutions Virtual Federal Image (VFI). Based on the Federal Information Processing Standard (FIPS) security categorization of "Moderate" (Confidentiality: Moderate, Integrity: Moderate, Availability: Moderate) and the FedRAMP Security Assessment Process[1], the JAB has determined that the VFI meets the information security requirements and is granted FedRAMP Provisional Authorization to Operate (P-ATO). Based on the third-party assessment conducted by Kratos SecureInfo, and review by the JAB, there are no outstanding high vulnerabilities.

The security authorization of the information system will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130, currently three years from the date of this letter, as long as:

1. Day1 Solutions satisfies the requirement of implementing continuous monitoring activities, as documented in FedRAMP's continuous monitoring requirements, and the VFI Continuous Monitoring Plan.
2. Day1 Solutions mitigates all open low and moderate POA&M action items, agreed to in the Security Assessment Report (SAR).
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies.

The Day1 Solutions VFI is delivered as an Infrastructure-as-a-Service (IaaS) offering using a multi-tenant community cloud computing environment. It is available to U.S. Federal, state, and local government entities.

[1] FedRAMP Security Assessment Process is available at www.fedramp.gov.

1800 F St NW
Washington, DC 20405
www.FedRAMP.gov

The VFI is a solution using an industry-leading virtualization technology leveraged upon a compliant IaaS environment. Day1 offers a simple, yet secure, IaaS environment with a robust IPS/IDS security border and best-in-class firewall, switching infrastructure, compute and storage devices. Using the secure access portal, the IaaS environment allows agencies at-will deployment of systems without any predetermined OS type or functionality of the image ("OS-agnostic"). This gives Federal, state, and local government customers the most flexible options possible in implementing their systems into Day1's government-only community cloud. Day1 Solutions replicates the entire VFI infrastructure elements at the Manassas, Virginia data center to an alternative processing site (data center) located centrally within the continental United States. All security controls are identical for both the primary and alternative processing centers, and both are fully operational at all times. The two processing centers are connected at all times by a dedicated private, multi-path 10GB network.

Federal Agencies are encouraged to leverage this FedRAMP P-ATO as a key element of their Authorization to Operate (ATO). Based on the FedRAMP Provisional Authorization to Operate and customer-specific tailoring and operating procedures, the JAB believes the FedRAMP Security Authorization Package accurately documents the VFI and clearly defines outstanding risk considerations.

Copies of the authorization package are available for review on the FedRAMP Security Authorization Package Repository. If you have any questions or comments regarding this Provisional Authorization to Operate, please contact Matthew Goodrich, FedRAMP Director, matthew.goodrich@gsa.gov, (202) 870-6231.

APPROVED:

X _____

Mr. Terry Halvorsen
Chief Information Officer
Department of Defense

1800 F St NW
Washington, DC 20405
www.FedRAMP.gov

Figure 5.4.1.2-2. Lumen's Teammate's IaaS P-ATO Letter (note-digital signatures were not able to be copied to proposal)

5.4.1.3 Overview of FedRAMP Test Plan

At any time, a Government agency can request the FedRAMP package from the GSA. Using the baseline for security controls within FedRAMP allows agencies to better focus on agency-specific requirements, and reduces certification and accreditation costs. The FedRAMP standards and processes leverage the work and initiatives of other federal agencies, as well as compliance statutes and programs. Agency ATOs can provide insights to other agencies, which can use this ATO information to help evaluate the scope and suitability of their own information security reviews. Beyond providing a common approach and requirements that streamline assessments, FedRAMP makes it easier and less costly for federal agencies to deploy new cloud services by standardizing and streamlining compliance assessments.

5.4.2 Test Scenario TS-02 [G.8]

Objective	Demonstrate that awarded services are delivered based on the KPIs and SLAs defined.
Approach	Lumen's approach is based on the test scenario for each service offered under the EIS contract as identified in this section 5.2.
Acceptance Criteria	Lumen will demonstrate that the service works properly according to KPIs defined in Section C.2.

5.4.2.1 Data Services [C.2.1]

5.4.2.1.1 Virtual Private Network Service [C.2.1.1.4]

Figure 5.4.2.1.1-1. TS-02-VPNS

Requirement	Descriptions
Verification & Acceptance Testing Approach	Dynamic verification to ensure that the contractor's Virtual Private Network Service (VPNS) provides secure, reliable transport of agency applications across the provider's high-speed unified multi-service IP-enabled backbone infrastructure. Lumen will complete test cases as identified in Figures 5.4.2.1.1-2 through 5.4.2.1.1-4 for the VPNS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and

Requirement	Descriptions
	procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	VPNS Provisioning Tests Requirements • The test should be performed on the Plant Test Date (PTD) from Lumen's demarc at the customer premise. • Customer location visits for testing will be prearranged with the customer if possible. • The customer should be informed that the circuit was tested and passed. An appropriate test will be completed to stress the transport media connecting the customer location to the Provider Edge (PE) router. To verify correct routing on IP VPN customer an addition ICMP echo request may be sent to the private IP of the customer edge router.

Figure 5.4.2.1.1-2. TEST CASE-VPNS-LAT

Requirement	Description
Parameters Measured	CONUS Latency (ms) OCONUS Latency (ms) Latency value is the average round trip transmission between agency premises routers for an IP VPN with its CONUS and OCONUS sites. Exclusion: Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods).
Measurement Procedure	As specified in RFC 1242 & RFC 2285
Acceptance Criteria	Routine Service Level (CONUS) ≤ 70 ms Routine Service Level (OCONUS) ≤ 150 ms

Figure 5.4.2.1.1-3. TEST CASE-VPNS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the agency. Computed by the standard formula: $Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$

Requirement	Description
Acceptance Criteria	Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%

Figure 5.4.2.1.1-4. TEST CASE-VPNS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.1.2 Ethernet Services [C.2.1.2.4]

Figure 5.4.2.1.2-1. TS-02-EthS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure that the provided Ethernet Services (EthS) allow agencies to interconnect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN) regardless of the geographical location of their sites. The following Ethernet services shall be tested - • Ethernet Private Line (E-LINE) - a point-to-point service in which bandwidth is reserved and used for mission critical traffic. E-Line supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different quality of service (QoS) priorities for customer traffic. • Ethernet Private LAN(E-LAN) - supports both point-to-multipoint and multipoint-to-multipoint configurations. It supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different QoS priorities for customer traffic. Lumen will complete test cases as identified in Figures 5.4.2.1.2-2 through 5.4.2.1.2-7 for the Ethernet Service verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that

Requirement	Description
	fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	Our Ethernet Service verification tests steps are as follows: • Layer 2 RFC 2544, which involves the following tests for both Optical and Wireline: o Throughput o Latency o Frame Loss Ratio o Back-to-Back Frames o Upon completion of the first test, all test results and screen shots are recorded. • For Optical, measure and verify Optical Levels: o Verify optical receive levels to ensure that they meet the specifications for the circuit terminating on the Lumen Network. • Ethernet Service Provisioning Testing: 1. The test is performed on the Plant Test Date (PTD) demarc to demarc. 2. Initial measurements made using EtherSAM to Layer 1 loopback (patch cord or port loopback) 3. If Loopback testing fails using EtherSAM, use Dual Test Sets (DTS) mode with EtherSAM for further analysis.

Figure 5.4.2.1.2-2. TEST CASE-EthS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Measured end-to-end and calculated as a percentage of the total reporting interval time that the EthS is operationally available to the agency. Computed by the standard formula: $Av(EthS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%

Figure 5.4.2.1.2-3. TEST CASE-EthS-LAT

Requirement	Description
Parameters Measured	CONUS Latency (ms) OCONUS Latency (ms)
Measurement Procedure	Latency is the round trip delay experienced by an end-user across the contractor's network to other agency's sites. It is the average time for packets to travel over the core network. As specified in RFC 1242 and RFC 2285. The Internet Control Message Protocol (ICMP) test

Requirement	Description
	consists of sending, every five minutes, a series of five test packets between originating agency's SDPs and the delivery SDPs. The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Latency can then be determined by the following formula: (Distance/(0.6*c)+hops*delay), where c is the velocity of light and 0.6 is the multiplier recommended by the ITU (G.144) in ms/km plus the delay in each hop caused by the routers times the number of hops.
Acceptance Criteria	CONUS ≤ 100 ms OCONUS ≤ 200 ms

Figure 5.4.2.1.2-4. TEST CASE-EthS-Jit

Requirement	Description
Parameters Measured	Packet jitter (ms)
Measurement Procedure	Packet jitter is the variation in latency as measured in the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. As specified in RFC 2679
Acceptance Criteria	Routine Service Level ≤ 10 ms

Figure 5.4.2.1.2-5. TEST CASE-EthS-GOS PDR

Requirement	Description
Parameters Measured	Packet delivery rate (%)
Measurement Procedure	Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. The loss can be measured with the ICMP test. As specified in RFC 1242 and RFC 2285.
Acceptance Criteria	Routine Service Level ≥ 99.95% at all times. Critical Service Level ≥ 99.99% at all times.

Figure 5.4.2.1.2-6. TEST CASE-EthS-GOS PL

Requirement	Description
Parameters Measured	Grade of Service (Packet Loss). Restoration for links transported over the Ethernet infrastructure
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Routine: Less than 1 minute Critical: Less than 100 ms

Figure 5.4.2.1.2-7. TEST CASE-EthS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.1.3 Optical Wavelength Service [C.2.1.3.4]

Figure 5.4.2.1.3-1. TS-02-OWS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure that the provided dedicated broadband, framing-independent transport networks are able to suitably interconnect agency offices in different regions of the United States and internationally. The method of providing OWS is Wavelength Division Multiplexing (WDM). OWS is provided over WDM equipment where several wavelengths, or lambdas, are multiplexed into a composite signal that is transported over a single fiber. The composite signal is then de-multiplexed at the receiver end and each wavelength is recovered. Lumen will complete test cases as identified in Figures 5.4.2.1.3-2 through 5.4.2.1.3-4 for the OWS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	<u>2.5G or 10G LAMBDA Provisioning Stress Testing:</u> • The stress test should be performed on the Plant Test Date (PTD) Demarc to Demarc. The test can be performed either with two test sets and running head-to-head from the point of Demarcation or with one test set to a f ber loopback at the point of Demarcation. • Customer location visits for stress testing will be prearranged with the customer if possible. <u>Required Provisioning Stress Tests for 2.5G or 10G LAMBDA:</u>

Requirement	Description
	• Bit Error Rate (BER) • Error Free Seconds • Line Code 40G or 10G LAMBDA Provisioning Stress Testing: 1. The stress and benchmark testing should be performed on the Plant Test Date (PTD) Demarc to Demarc. The test will be performed with one test set to a fiber loopback at the point of Demarcation. 2. Customer location visits for testing will be prearranged with the customer if possible. 3. The customer should be informed that the circuit was stressed and did pass with zero errored seconds. Required Provisioning Stress Tests for 40G or 100G LAMBDA There are two tests required: 1. RFC2544 test to capture a MTU spread and Latency baseline. 2. EtherBERT test to stress test the pipe. RFC2544 Use all default settings except for the following: 1) Frame Size distr bution = User Defined, change 1518 Frame size to 9216 2) Set Trial duration for Throughput, Frame Loss and Latency to 00:10 seconds

Figure 5.4.2.1.3-2. TEST CASE-OWS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	OWS availability shall be measured in service on an end-to-end basis. COT(HR) shall be calculated based on ES and/or SES as defined by GR-253, G.826 through G.829 and expressed in hours. Availability is computed by the standard formula: $Av(OWS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%

Figure 5.4.2.1.3-3. TEST CASE-OWS-GOS

Requirement	Description
Parameters Measured	Restoration time (ms)
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Routine Service Level ≤ 100 ms Critical Service Level ≤ 60 ms

Figure 5.4.2.1.3-4. TEST CASE-OWS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.1.4 Private Line Service [C.2.1.4.4]

Figure 5.4.2.1.4-1. TS-02-PLS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure the provisioned PLS provides dedicated, reliable full duplex bandwidth for agency-specific data networks and mission critical applications. The PLS must enable dedicated duplex transmission connectivity between two or more designated end points over which agency service applications traverse at agency- specified bandwidths. Lumen will complete test cases as identified in Figures 5.4.2.1.4-2 through 5.4.2.1.4-3 for the PLS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	Our PLS verification tests steps are as follows: • Identify access point of circuit • Determine line code for the appropriate tests • Remotely loop device at the A and Z end of the circuit termination to validate remote loop back is operational • Run the following end-to-end service activation tests: • Transmit F2^23-1 pattern

Requirement	Description
	• If test fails, troubleshoot and resolve • Record all test results and test result screen shots • End-to-end testing will be performed when specified in the service order.

Figure 5.4.2.1.4-2. TEST CASE-PLS-Av

Requirement	Description	
Parameters Measured	Availability (%) for: • POP to POP (optional) • SDP to SDP For data rates of T1 and higher, a service is considered unavailable when a PLS circuit experiences 10 consecutive severely errored seconds (SES) [Standard: Telcordia PUB GR-418-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds to account for stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time. For data rates lower than T1, cumulative outage time is calculated based on trouble ticket data. PLS availability is calculated as a percentage of the total reporting interval time that PLS is operationally available to the agency.	
Measurement Procedure	Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100.$	
Acceptance Criteria	POP to POP: Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%	SDP to SDP: Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%

Figure 5.4.2.1.4-3. TEST CASE-PLS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.1.5 Synchronous Optical Network Services [C.2.1.5.4]

Figure 5.4.2.1.5-1. TS-02-SONET

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure the provisioned SONETS supports a wide range of digital signals with different capacities, and its interworking capability enables seamless communications between devices that support dissimilar protocols such as IP, Frame Relay, and ATM. SONETS enables agencies to transport voice, data, and video throughout the United States and internationally. SONETS services shall connect to and interoperate with: Government specified terminations (e.g., SDP-to-SDP, POP-to-POP). All other networks including other EIS contractors' networks where industry standards are used. Lumen will complete test cases as identified in Figures 5.4.2.1.5-2 through 5.4.2.1.5-3 for the SONET verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.

Test Setup	SONET service verification tests steps are as follows:
	• Identify access point of circuit
	• Set-up Bit Error Test Set (Our SONET services are tested using a variety of Digital Lightwave and JDSU testing products)
	• Remotely loop device at the A and Z end of the circuit termination to validate remote loop back and perform initial continuity test
	• Release loop remotely/normalize circuit
	• Run the following end-to-end service activation tests:
	  o Working Channel
	  o Protect Channel
	• If test fails, troubleshoot and resolve
	• Record all test results and test result screen shots

Figure 5.4.2.1.5-2. TEST CASE-SONET-Av

Requirement	Description
Parameters Measured	Availability SDP-to-SDP (%)
Measurement Procedure	SONETS availability shall be measured in-service and on an end-to-end basis. COT(HR) shall be calculated based on ES and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula: $Av(SONETS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.8% Critical Service Level ≥ 99.999%

Figure 5.4.2.1.5-3. TEST CASE-SONET-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.1.6 Internet Protocol Service [C.2.1.7.4]

Figure 5.4.2.1.6-1. TS-02-IPS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure that the provisioned Internet Protocol Service (IPS) supports a wide range of connectivity requirements that enable Government users to access the Internet, Government-wide intranets, and extranets. IPS will use the TCP/IP protocol suite to interconnect GFE/SRE with other Government networks and the public Internet Service Provider (ISP) networks. Lumen will complete test cases as identified in Figures 5.4.2.1.7-2 through 5.4.2.1.7-5 for the IPS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Traffic simulate could include: • Time-critical traffic (such as voice and video); • Business-critical traffic (such as transactions); and • Non-critical traffic (such as email).

Requirement	Description
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	VPNS Provisioning Tests Requirements: • The test should be performed on the Plant Test Date (PTD) from Lumen's demarc at the customer premise. • Customer location visits for testing will be prearranged with the customer if possible. • The customer should be informed that the circuit was tested and passed. An appropriate test will be completed to stress the transport media connecting the customer location to the Provider Edge (PE) router. To verify correct routing on IP VPN customer an addition ICMP echo request may be sent to the private IP of the customer edge router. Dependent upon access service type once the transport section has been verified via the Test Data Set and customer equipment has been connected a final ICMP echo host request will be sent from the provider edge router to the public IP of the customer edge router to verify layer 3 connectivity.

Figure 5.4.2.1.6-2. TEST CASE-IPS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula: $Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.95% Critical Service Level ≥ 99.995%

Figure 5.4.2.1.6-3. TEST CASE-IPS-LAT

Requirement	Description
Parameters Measured	Latency (ms)—Latency is the backbone delay experienced across the EIS network. It is the average time for IP packets to travel over the EDIS core network. The Backbone Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods.
Measurement Procedure	The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets

Requirement	Description
	between EIS core service aggregation points (i.e., POPs). The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Relevant standards: RFC 1242 and RFC 2285.
Acceptance Criteria	Routine Service Level ≤ 60 ms Critical Service Level ≤ 50 ms

Figure 5.4.2.1.6-4. TEST CASE-IPS-GOS

Requirement	Description
Parameters Measured	Data Delivery Rate (%)
Measurement Procedure	Network packet delivery is a measure of IP packets successfully sent and received over the EIS core network. The data delivery rate can be measured with the ICMP test.
Acceptance Criteria	Routine Service Level ≥ 99.9% Critical Service Level ≥ 99.99%

Figure 5.4.2.1.6-5. TEST CASE-IPS-TTR.

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.2 Voice Services [C.2.2]

5.4.2.2.1 Internet Protocol Voice Service [C.2.2.1.4]

Figure 5.4.2.2.1-1. TS-02-IPVS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure the provisioned IPVS provides voice communications service and telephony features to agencies using VoIP over a managed IP network. IPVS supports voice calls, whether initiated from on-net locations or from off-net locations, to be connected to all on-net and off-net locations by direct station-to-station dialing. Lumen will complete test cases as identified in Figures 5.4.2.2.1-2 through 5.4.2.2.1-7 for the IPVS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for

Requirement	Description
	service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Toolset will simulate network traffic.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	RFC 2544 Testing of transport layer: All RFC 2544 test parameters should be adjusted to accommodate the business decision implicit in calculating the duration of the total test scenario. • Throughput • Latency • Packet Jitter • Frame Loss • Back to Back During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include validate of the service features.

Figure 5.4.2.2.1-2. TEST CASE-IPVS-LAT

Requirement	Description
Parameters Measured	Latency (ms)
Measurement Procedure	Latency is the average round trip time for a packet to travel from source SDP to destination SDP. This applies to CONUS.
Acceptance Criteria	Routine Service Level ≤ 200 ms

Figure 5.4.2.2.1-3. TEST CASE-IPVS-GOS

Requirement	Description
Parameters Measured	Packet Loss (%)
Measurement Procedure	Grade of Service (Packet Loss) is defined as the percentage of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped). The packet loss can be measured with an ICMP test. This applies to CONUS.
Acceptance Criteria	Routine Service Level ≤ 0.4%

Figure 5.4.2.2.1-4. TEST CASE-IPVS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the IPVS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.6% Critical Service Level ≥ 99.9%

Figure 5.4.2.2.1-5. TEST CASE-IPVS-Jit

Requirement	Description
Parameters Measured	Jitter (ms)
Measurement Procedure	Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS.
Acceptance Criteria	Routine Service Level ≤ 10 ms

Figure 5.4.2.2.1-6. TEST CASE-IPVS-VQ

Requirement	Description
Parameters Measured	Voice Quality is measured by the Mean Opinion Score (MOS)
Measurement Procedure	As defined in ITU-T specification P.800 series.
Acceptance Criteria	Routine MOS ≥ 4.0

Figure 5.4.2.2.1-7. TEST CASE-IPVS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.2.2 Circuit Switched Voice Service [C.2.2.2.4]

Figure 5.4.2.2.2-1. TS-02-CSVS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure the provisioned CSVS provides voice communications service and telephony features to agencies. CSVS supports voice calls, whether initiated from on-net locations or from off-net locations, to be connected to all on-net and off-net locations by direct station-to-station dialing. Lumen will complete test cases as identified in Figures 5.4.2.2.2-2 through 5.4.2.2.2-4 for the CSVS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Toolset will simulate network traffic.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include: o LD call o Local call o Call forwarding o Toll free call o Inbound call o Call transfer o Failover routing if applicable • Testing for validation of service features

Figure 5.4.2.2.2-2. TEST CASE-CSVS-Av

Requirement	Description
Parameters Measured	Availability (POP-to-POP) Availability (SDP-to-SDP) Exclusion: Note that this KPI is waived for calls made with calling card.
Measurement Procedure	CSVS availability is calculated as a percentage of the total reporting interval time that the voice service is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$

Requirement	Description	
Acceptance Criteria	POP-to-POP Routine Service Level ≥ 99.95%	SDP-to-SDP Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.95%

Figure 5.4.2.2.2-3. TEST CASE-CSVS-GOS

Requirement	Description	
Parameters Measured	Call Blockage (ratio)	
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.	
Acceptance Criteria	POP-to-POP: Routine Service Level ≤ 0.01 Critical Service Level ≤ 0.01	SDP-to-SDP: Routine Service Level ≤ 0.07 Critical Service Level ≤ 0.01

Figure 5.4.2.2.2-4. TEST CASE-CSVS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.2.3 Toll Free Service [C.2.2.3.4]

Figure 5.4.2.2.3-1. TS-02-TFS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.2.3-2 through 5.4.2.2.3-4 for the TFS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Toolset will simulate network traffic.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.

Requirement	Description
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include: o Toll free call o Testing for validation of service features including basic inbound toll free calling, advanced feature and call routing capabilities, intelligent call routing and network-based Interactive Voice Response (IVR) capabilities.

Figure 5.4.2.2.3-2. TEST CASE-TFS-Av

Requirement	Description	
Parameters Measured	Availability (POP-to-POP)	Availability (POP-to-SDP)
Measurement Procedure	Av (POP-to-POP) and Av (POP-to-terminating SDP) are measured and calculated as a percentage of the total reporting interval time that TFS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$	
Acceptance Criteria	POP-to-POP Routine Service Level ≥ 99.95%	POP-to-SDP Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.95%

Figure 5.4.2.2.3-3. TEST CASE-TFS-GOS

Requirement	Description
Parameters Measured	Call Blockage (ratio)
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Routine Service Level ≤ 0.07 Critical Service Level ≤ 0.01

Figure 5.4.2.2.3-4. TEST CASE-TFS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.2.4 Circuit Switched Data Service [C.2.2.4.4]

Figure 5.4.2.2.3-1. TS-02-CSDS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.2.3-2 through 5.4.2.2.3-4 for the CSDS verification and acceptance testing.
Test Dataset	Lumen uses and deploys industry standard commercial best practices and test equipment for service test and acceptance. As an adopter of best commercial practices as technology refreshes and procedures change Lumen adjusts our processes accordingly. Upon contract award Level3 would be pleased demonstrate these tools and practices. Toolset will simulate network traffic.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include: o Initial Data Call set up o Initial Data Call completion o Validate data channel bonding for specified bandwidth o Testing for validation of service features including dial-in and user-to-user signaling

Figure 5.4.2.2.3-2. TEST CASE-CSDS-Av

Requirement	Description	
Parameters Measured	Availability (POP-to-POP)	Availability (SDP-to-SDP)
Measurement Procedure	CSDS availability is calculated as a percentage of the total reporting interval time that CSDS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$	
Acceptance Criteria	POP-to-POP Routine Service Level ≥ 99.95%	SDP-to-SDP Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.95%

Figure 5.4.2.2.3-3. TEST CASE-CSDS-GOS

Requirement	Description	
Parameters Measured	Call Blockage (ratio)	
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.	
Acceptance Criteria	POP-to-POP: Routine Service Level ≤ 0.01 Critical Service Level ≤ 0.01	SDP-to-SDP: Routine Service Level ≤ 0.07 Critical Service Level ≤ 0.01

Figure 5.4.2.2.3-4. TEST CASE-CSDS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.3 Contact Center Services [C.2.3]

5.4.2.3.1 Contact Center Services [C.2.3.1.4]

Figure 5.4.2.3.1-1. TS-02-CCS

Requirement	Description

Requirement	Description
Verification & Acceptance Testing Approach	Static verification to ensure the provided Contact Center Services can enable subscribing agencies to deliver customer service to their designated customer base across multi-media contact channels (voice, fax, email, Internet website, etc.) and provide additional enabling services for end to end customer service. The basic service must provide intelligent call routing capabilities with a network call queue. The CCS will apply to single site, multiple site, and enterprise wide agency contact centers. Lumen will complete test cases as identified in Figures 5.4.2.3.1-2 through 5.4.2.3.1-3 for the CCS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features depending on which service delivery methods for CCS is contracted by the agency. • Host Based Call Management Service. Lumen providing the necessary components required for CCS Call Management Service. • Premises Based Call Management Service. Lumen providing the necessary components required for CCS Call Management Service to be located at an agency provided location. • Premises Based Call Answering Service. • Host Based Call Answering Service. Lumen providing personnel located and perform operations at a contractor provided location

Figure 5.4.2.3.1-2. TEST CASE-CCS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.9%

Figure 5.4.2.3.1-3. TEST CASE-CCS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.4 Colocated Data Center Services [C.2.4]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.5 Cloud Services [C.2.5]

5.4.2.5.1 Cloud Services [C.2.5.1.4, C.2.5.2.4, C.2.5.3.4]

Figure 5.4.2.5.1-1. TS-02-IaaS-PaaS-SaaS

Requirement	Description
Verification & Acceptance Testing Approach	Static & dynamic verification to confirm compliance with technical standards as specified in Section C.2.5.1.1.2. The Platform as a Service (PaaS) offerings will facilitate deployment of software applications in the cloud without the cost and complexity of buying and managing the underlying hardware, software, and provisioning hosting capabilities. PaaS provides complete software platforms, including capabilities such as databases, DBMSs, developer tools, testing tools, and directory services. Using PaaS, software developers can build, test, and deploy custom application quickly at a low cost. Software as a Service (SaaS) allows software and applications to be hosted in the cloud and accessed by users via, for example, agency intranet. SaaS will host enterprise business applications, such as accounting, collaboration, customer relationship management, enterprise resource planning, and many more. Lumen will complete test cases as identified in Figures 5.4.2.5.1-2 through 5.4.2.5.1-3 for the Cloud Services verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include

Requirement	Description
	the testing for validation of service features.

Figure 5.4.2.5.1-2. TEST CASE-IaaS-PaaS-SaaS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	IaaS Data Center Infrastructure availability is calculated as a percentage of the total reporting interval time that the IaaS Data Center Infrastructure is operationally available to the agency. Availability is computed by the standard formula: $Av(Datacenter) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$ The scheduled maintenance windows are excluded from the availability calculation.
Acceptance Criteria	Routine Service Level ≥ 99.95%

Figure 5.4.2.5.1-3. TEST CASE-IaaS-PaaS-SaaS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.3.5.2 Content Delivery Network Service [C.2.5.4.4]

Figure 5.4.2.5.2-1. TS-02-CDNS

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure the provisioned Content Delivery Network Service (CDNS) efficiently and rapidly deliver agency's content to Web browsers Worldwide. The CDNS provider will incorporate equipment and algorithms to cache content on geographically dispersed servers on the Internet. When a request is made from a particular location for specific content, the server that can most rapidly and efficiently provide the content is dynamically identified. Lumen will complete test cases as identified in Figures 5.4.2.5.2-2 through 5.4.2.5.2-4 for the CDNS verification and acceptance testing.

Requirement	Description
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	Lumen Team will verify that individual services delivered function at acceptable and contractually established performance levels. Our procedures include random, unscheduled testing of each vendor's services, either directly with our own test suite, or under contract with testing organizations. This ensures that our services are operating as required and that any out-of-bound performance ratios are corrected immediately. Random URLs tested; once a week at a random time during a 24-hour period, selecting both US and international client Web sites. Day, start time, and end time are all random. Lumen Team measures connection times, rebuffer times, buffer times, and stream quality. Following each test cycle detailed reports indicating the testing procedures are used to verify the level of service; whether performance was acceptable; and whether KPI/AQL compliance was maintained.

Figure 5.4.2.5.2-2. TEST CASE-CDNS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	CDNS availability is calculated as a percentage of the total reporting interval time that the CDNS is operationally available to the agency. Availability is computed by the standard formula: $Av(CDNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level = 99.99%

Figure 5.4.2.5.2-3. TEST CASE-CDNS-GOS

Requirement	Description
Parameters Measured	Time to refresh content (min)
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Routine Service Level ≤ 5 min

Figure 5.4.2.5.2-4. TEST CASE-CDNS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.6 Wireless Services [C.2.6]

Figure *5.4.2.6-1.* TS-02-WIRELESS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.6.1-2 through 5.4.2.6.1-3 for the Wireless Services verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	Wireless Service shall connect to and interoperate with the following: 1. The Public Switched Telephone Network (PSTN) and the world wide dialing plan per ITU Recommendation E.164. 2. Originate and terminate calls to users of commercial satellite-based services. 3. The Internet. 4. Agency mobile terminals, such as, but not limited to cellular phones, smartphones, wireless-enabled Notebook and Laptop PCs, and PDAs.

Figure *5.4.2.6-2.* TEST CASE-WS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	1. MWS availability is calculated based on availability of access to the contractor's network from the contractor's cell site. 2. Radio access network performance is likely to vary depending on location (e.g., urban, suburban, or rural), as well as the technical specifications and capabilities of the deployed infrastructure, such as the radio access equipment.

Requirement	Description
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure *5.4.2.6-3.* TEST CASE-WS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: ≤4 hours With Dispatch: ≤8 hours

Figure 5.4.*2.6*-4. Test Validation Steps

Managed Wireless Service Verification			
Step #	**Action**	**Expected Result**	**Actual Result**
1	Customer Order Verification	Review of customer order by Dedicated Federal Wireless Order Group meets customer requirements as specified by Lumen and its WMS Vendor's Customer Account Team.	
2(a)	Voice Service Verification	Customer can successfully send and receive voice calls.	
2(b)	Data Service Verification	Customer can successfully send and receive SMS messages and access the public internet. NOTE: If VPNS gateway is ordered via the Service order that the device only connects to the enterprise instance.	

5.4.2.7 Commercial Satellite Communications Services [C.2.7]

Figure 5.4.2.7.1-1. TS-02-COMSATCOM

Requirement	Description
Verification & Acceptance Testing Approach	Dynamic verification to ensure that the provisioned COMSATCOM provide end-to-end mobile or fixed commercial satellite communications (COMSATCOM) services to include, but not be limited to, contractor provided earth terminals, satellite bandwidth, radio frequency equipment, satellite phones, interfaces and support systems, as identified in TOs. Lumen will complete test cases as identified in Figures 5.4.2.7.1-2 through 5.4.2.7.1-7 for the COMSATCOM verification and acceptance testing.
Test Dataset	JDSU T-BERD 6000A w/ Multi-Services Applications Module (MSAM)

Requirement	Description
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	Satellite Modem-to-Modem Testing 1. Technician will confirm test set equipment is properly calibrated and in good working condition prior to arriving onsite. 2. Test Duration: 72 Hours 3. Ensure test cables and connectors are in good working condition for proper Transmit and Receive Data. 4. Ensure end-to-end connectivity by sending and properly receiving five (5) bit errors. Test Prestart: (1) Insert tester interface cable into the distribution patch. (2) Coordinate with distant end technician to initiate test. (3) Observe "SYNC" indicator is lit. Test Initiation: Site technicians will periodically monitor test measurements throughout the end-to-end test. If site access is not an issue, measurement checks will be performed every eight hours. If errors are recorded, the CPMO will schedule a conference call with all parties to begin immediate troubleshooting. Test Conclusion: Field Engineers will capture and submit the test results to the designated Government Program Manager or COR for commissioning evaluation. Ethernet Port Testing The JDSU 6000A test set provides testing at three layers, layer 1, layer 2, and layer 3. Layer 1 is the physical bits and blocks of Ethernet protocol. Layer 1 tests verify the physical characteristics over a single wire between two ports. Layer 2 is the addressed frame level. Layer 2 tests verify the frame integrity in a switched network. Layer 3 is the packet layer or IP layer testing, and verifies packet applications such as Ping. 10/100/1G BaseT Half Duplex Layer 2 or Switched Ethernet Port Testing 1. Verify the test results. Record test results and duration. 2. The Summary category automatically displays error results. 3. Select the port and then the L2 Bert Stats category display to see the following statistics: • Test length • Availability • Error Free Seconds • Severely Errored Seconds • Degraded Minutes • Mean Time To Loss of BCI • Delay (one way) Serial Line, RS-530 Testing

Requirement	Description
	T-BERD 6000A provides RS-232/V.24, EIA-530, MIL-188c, V.35, RS-449/v.36, and MIL188-114 interfaces. Field test is focused on RS-530 serial line BERT. 1. EIA-530 BERT DTE 1.536 Mbps 2. EIA-530 BERT DCE 1.536 Mbps Connect the Test set for RS-232/V.24, and EIA-530 testing using a DISN-02, DB-25 cable. Before testing RS-232/V.24, and EIA-530 interfaces, you connect the Test Set to the circuit using a DB-25 cable with male connectors and the DB-25 connector on the top panel. To connect for RS-232/V.24, and EIA-530 testing: 1. Connect one end of the DB-25 cable to the DB-25 connector on the top panel of the test set. 2. Connect the opposite end of the DB-25 cable to the circuit under test Verify Results OK displays. Record test results and duration.

Figure 5.4.2.7.1-2. TEST CASE-COMSATCOM-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	CFSS and CMSS availability is calculated as a percentage of the total reporting interval time that they are operationally available to the agency. Availability is computed by the standard formula: $Av\ (CFSS\ \ \&\ CMSS\ ) = \frac{RI\ (HR\ ) - COT\ \ (HR\ )}{RI\ (HR\ )} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure 5.4.2.7.1-3. TEST CASE-COMSATCOM-EFS

Requirement	Description
Parameters Measured	Error Free Seconds
Measurement Procedure	See Test Setup
Acceptance Criteria	Routine Service Level > 0.965

Figure 5.4.2.7.1-4. TEST CASE-COMSATCOM-SES

Requirement	Description
Parameters Measured	Severely Errored Seconds
Measurement Procedure	See Test Setup

Acceptance Criteria	Routine Service Level ≤ 0.0003

Figure 5.4.2.7.1-5. TEST CASE-COMSATCOM-DM

Requirement	Description
Parameters Measured	Degraded Minutes
Measurement Procedure	See Test Setup
Acceptance Criteria	Routine Service Level ≤ 0.02

Figure 5.4.2.7.1-6. TEST CASE-COMSATCOM-MTTLBCI

Requirement	Description
Parameters Measured	Mean Time To Loss of BCI (MITTBCI)
Measurement Procedure	See Test Setup
Acceptance Criteria	Routine Service Level ≥ 24 hours

Figure 5.4.2.7.1-7. TEST CASE-COMSATCOM-Delay

Requirement	Description
Parameters Measured	Delay (one way)
Measurement Procedure	See Test Setup
Acceptance Criteria	The lesser of 450 msec or (260 + 0.01 x D ms) "D" is the SDP to SDP transmission distance, measured shortest great circle, in kilometers.

5.4.2.8 Managed Services [C.2.8]

5.4.2.8.1 Managed Network Service [C.2.8.1.4]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.8.2 Web Conferencing Service [C.2.8.2.4]

Figure 5.4.2.8.2-1. TS-02-WCS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.2-2 through 5.4.2.8.2-3 for the WCS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features.

Figure 5.4.2.8.2-2. TEST CASE-WCS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Availability is measured and calculated as a percentage of the total reporting interval time that WCS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.9%

Figure 5.4.2.8.2-3. TEST CASE-WCS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.3 Unified Communication Service [C.2.8.3.4]

Figure 5.4.2.8.3-1. TS-02-UCaaS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.3-2 through 5.4.2.8.3-3 for the UCaaS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features.

Figure 5.4.2.8.3-2. TEST CASE-UCaaS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Availability is measured and calculated as a percentage of the total reporting interval time that UCS is operationally available to the agency. $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure 5.4.2.8.3-3. TEST CASE-UCaaS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.4 Managed Trusted Internet Protocol Service [C.2.8.4.4]

Figure 5.4.2.8.4-1. TS-02-MTIPS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will verify MTIPS before handing new services over to the agency. Lumen will ensure the service is performing to the specifications of the KPIs as noted in Figures 5.4.2.8.4-2 through 5.4.2.8.4-9 and functionality of the service features in accordance with EIS RFP Section C.2.8.4. the test suites are examples. Final test suites to be negotiated and mutually agreed upon by Lumen GSA and DHS.
Test Dataset	Test datasets will be used based on the testing attr butes identified in the test setup section.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	The Lumen technician performs the following testing activities based on the agency's MTIPS service order specifications. • The transport layer (MPLS/IPVPN depending on the service order) is tested based on appropriate type of access methodology following RFC 2544 test parameters. • The cross connects between the MTIPS gateway and the agency's environment will be tested. • Connective testing of the VLAN. • Testing of the MTIPS Enclave Edge Firewall setting based on agency defined rules which could include: o Mail records o Antivirus settings o Intrusion protection settings o Firewall ruleset (outer and inner) o Host settings o Web content settings o URL blocking settings o AV and banned word email filter settings o Application control settings o DLP settings o DMZ – VPN tunnel • The MTIPS port ingress/egress assurance testing for full throughput (port and speed) as ordered by the agency.

Figure 5.4.2.8.4-2. TEST CASE-MTIPS (TIC Portal)-Av

Requirement	Description
Parameters Measured	Availability (%) (TIC Portal) Note: Availability is measured during the test and acceptance period does not include down time due to any service modifications necessary to support customer activation.
Measurement	Availability is measured and calculated as a percentage of the total reporting interval time that TIC

Procedure	Portal is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.995%

Figure 5.4.2.8.4-3. TEST CASE-MTIPS (TIC Portal)-EN

Requirement	Description	Acceptance Criteria
Parameters Measured and Acceptance Criteria	Firewall Security Event Notification--The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the agency. Events are categorized as follows: Low – Events in the Low category have a negligible impact on service. They include incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems. Medium – Events in the Medium category have a more serious impact on service, and may indicate a poss ble security breach, threat or attack attempt. They may also cause the service to operate in a degraded state. High – Events in the High category represent violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, which should be immediately reported via email, or telephone, as specified by the agency.	≤ 24 hours of a low category event ≤ 4 hours of a medium category event ≤ 30 minutes of a high category event
	Intrusion Detection/ Prevention Security Event Notification Event Notification The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the agency. Events are categorized as above.	≤ 24 hours of a low category event ≤ 10 minutes of a high category event
Measurement Procedure	Not Applicable for service verification testing. MTIPS EN can only be tested upon service activation and a failover occurs.	

Figure 5.4.2.8.4-4. TEST CASE-MTIPS (TIC Portal)-GOS

Requirement	Description	Acceptance Criteria
Parameters Measured and Acceptance Criteria	The Grade of Service (Failover Time) for the TIC Portal is the time that it takes to switch from one TIC Portal instance to another provided by the same contractor.	Routine Service Level: ≤ 1 minute
	The GOS (Monitoring and Correlation) – The monitoring and correlation agents in the contractor's SOC shall detect a security event within 4 hours of its initiation at (a) 90% AQL for Routine, and (b) 99.9% AQL for Critical service	Routine Service Level: ≤ 5 hours 90% of the time Critical Service Level: ≤ 4

Requirement	Description	Acceptance Criteria
	levels. The monitoring and correlation systems shall provide real time fusion.	hours 99.9% of the time
	The GOS (Configuration/Rule Change) value represents the elapsed time between the configuration/change request and the change completion. The value is measured by logs/reporting. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).	≤ 5 hours for a normal priority change ≤ 2 hours for an urgent priority change
	The GOS (Virus Protection Updates and Bug Fixes) represents the time between the release of the virus protection updates and bug fixes (patches), and their deployment. This indicator ensures automatic and timely delivery of updates/bug fixes.	≤ 24 hours for a normal priority update ≤ 2 hours for an urgent priority update
Measurement Procedure	Not Applicable for service verification testing. MTIPS GOS can only be tested upon service activation and a failover occurs.	

Figure 5.4.2.8.4-5. TEST CASE-MTIPS (Collection/Distro)-Av

Requirement	Description
Parameters Measured	Availability (%) (Transport Collection and Distribution)
Measurement Procedure	Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.995%

Figure 5.4.2.8.4-6. TEST CASE-MTIPS (Collection/Distro)-Lat

Requirement	Description
Parameters Measured	Latency (CONUS)
Measurement Procedure	Latency is the average one-way time for IP packets to travel over the EIS core network. The Backbone Latency metric does not apply for DSL and Cable High Speed access methods.
Acceptance Criteria	Routine Service Level: ≤ 60 ms Critical Service Level: ≤ 50 ms

Figure 5.4.2.8.4-7. TEST CASE-MTIPS (Collection/Distro)-GOS

Requirement	Description
Parameters Measured	Data Delivery Rate
Measurement Procedure	Network packet delivery is a measure of IP packets successfully sent and received over the EIS core network.
Acceptance Criteria	Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.995%

Figure 5.4.2.8.4-8. TEST CASE- MTIPS (Collection/Distro)-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Time to restore service to normal upon receipt
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

Figure 5.4.2.8.4-9. TEST CASE-MTIPS (Collection/Distro)-EN

Requirement	Description
Parameters Measured	Security Incident Reporting
Measurement Procedure	Security incident reporting to DHS US-CERT must be performed in near real-time, congruent with NIST SP 800-61 Rev 2), not to exceed 30 minutes, from the time of detection.
Acceptance Criteria	Not Applicable. Response times can only be tested upon service activation.

5.4.2.8.5 Managed Security Service [C.2.8.5.4]

Figure 5.4.2.8.5-1. TS-02-MSS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.5-2 through 5.4.2.8.5-6 for the MSS verification and acceptance testing.
Test Dataset	Test datasets will be used based on the testing attributes identified in the test setup section.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.

Test Setup	The Lumen technician performs the following testing activities based on the agency's MSS service order specifications. • The transport layer (depending on the service order) is tested based on appropriate type of access methodology following RFC 2544 test parameters. • Testing of the connectivity into the agency environment where MSS will be delivered to ensure visibility. • Similar to the MTIPS feature testing, Lumen will verify the appropriate attr butes are performing to specification based on the service elements contracted at the Task Order level. MSS is comprised of the following underlying functions: o Managed Prevention Service o Vulnerability Scanning Service o Incident Response Service

Figure 5.4.2.8.5-2. TEST CASE-MSS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Percentage of the total reporting interval time that the Managed Security Services is operationally available to the agency.
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure 5.4.2.8.5-3. TEST CASE-MSS-EN

Requirement	Description
Parameters Measured	The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows: Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems. Medium — Events in the Medium category have a more serious impact on service, and may indicate a poss ble security breach, threat or attack attempt. They may also cause the service to operate in a degraded state. High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.
Measurement Procedure	Not Applicable. Event Notification times can only be tested upon service activation.

Requirement	Description	
Acceptance Criteria	For MPS: Routine—Less than or equal to 10 minutes	For INRS: Low Category Event: Before next business day or less than 24 hours Medium Category Event: Less than or equal to 4 hours High Category Event: Less than or equal to 1 hour

Figure 5.4.2.8.5-4. TEST CASE-MSS-GOS

Requirement	Description
Parameters Measured	The Grade of Service (Configuration Change, virus updates) value represents the elapsed time between the configuration change request and the change completion. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
Measurement Procedure	Not Applicable. Configuration Changes can only be tested upon service activation.
Acceptance Criteria	Normal priority change: Less than 5 hours for MFS (Managed Firewall) and less than 24 hours for VSS (Vulnerability Scanning) Urgent priority change: Less than or equal to 2 hours

Figure 5.4.2.8.5-5. TEST CASE-MSS-IRT

Requirement	Description	
Parameters Measured	1. Incident Response Time (Telephone) 2. Incident Response Time (On-Site) Elapsed time between the agency's notification to the contractor, and the contractor's implementation of response procedures, including arrival to affected site.	
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.	
Acceptance Criteria	Telephone: Low Category Event: Less than 1 hour High Category Event: Less than 15 min	On site: Low Category Event: Less than 36 hours Low Category Event: Less than 24 hours

Figure 5.4.2.8.5-6. TEST CASE-MSS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.

Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.6 Managed Mobility Service [C.2.8.6.4]

Figure 5.4.2.8.6-1. TS-02-MMS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.6-2 through 5.4.2.8.6-6 for the MMS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features.

Figure 5.4.2.8.6-2. TEST CASE-MMS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Percentage of the total reporting interval time that the Managed Mobility Service is operationally available to the agency
Acceptance Criteria	Routine Service Level ≥ 99.5% Critical Service Level ≥ 99.9%

Figure 5.4.2.8.6-3. TEST CASE-MMS-EN

Requirement	Description
Parameters Measured	Elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows: a) Low — Events in the Low category have a neglig ble impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems. b) Medium — Events in the Medium category have a more serious impact on service, and may

Requirement	Description
	indicate a poss ble security breach, threat or attack attempt. They may also cause the service to operate in a degraded state. c) High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.
Measurement Procedure	Not Applicable. Event notification times can only be tested upon service activation.
Acceptance Criteria	Low category event: Next business day or Less than 24 hours Medium category event: Less than 4 hours High category event: Less than 30 minutes

Figure 5.4.2.8.6-4. TEST CASE-MMS-GOS

Requirement	Description
Parameters Measured	Elapsed time between the configuration change request and the change completion.
Measurement Procedure	Not Applicable. Configuration change request times can only be tested upon service activation.
Acceptance Criteria	Normal Priority change: Less than 5 hours High Priority change: Less than 2 hours

Figure 5.4.2.8.6-5. TEST CASE-MMS-IRT

Requirement	Description	
Parameters Measured	Incident Response Time (Telephone) Incident Response Time (On-Site) Elapsed time between the agency's notification to the contractor, and the contractor's implementation of response procedures, including arrival to affected site.	
Measurement Procedure	Not Applicable. Incident response times can only be tested upon service activation.	
Acceptance Criteria	Telephone: Low Category Event: Less than 1 hour High Category Event: Less than 15 minutes	On site: Low Category Event: Less than 36 hours High Category Event: Less than 24 hours

Figure 5.4.2.8.6-6. TEST CASE-MMS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.

Requirement	Description
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.7 Audio Conferencing Service [2.8.7.4]

Figure 5.4.2.8.7-1. TS-02-ACS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.7-2 through 5.4.2.8.7-4 for the ACS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features.

Figure 5.4.2.8.7-2. TEST CASE-ACS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Percentage of the total reporting interval time that ACS is operationally available to the agency $Availabili\ ty = \frac{RI\,(HR) - COT\,(HR)}{RI\,(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure 5.4.2.8.7-3. TEST CASE-ACS-GOS

Requirement	Description
Parameters Measured	Delay experienced by conference participants to receive operator assistance during a conference.

Requirement	Description
Measurement Procedure	Delay is measured as the interval between the end of signaling (e.g., dialing for operator assistance) and the receipt of voice response from the operator.
Acceptance Criteria	Less than or equal to 30 seconds

Figure 5.4.2.8.7-4. TEST CASE-ACS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.8 Video Teleconferencing Service [C.2.8.8.4]

Figure 5.4.2.8.8-1. TS-02-VTS

Requirement	Description
Verification & Acceptance Testing Approach	Lumen will complete test cases as identified in Figures 5.4.2.8.8-2 through 5.4.2.8.8-4 for the VTS verification and acceptance testing.
Test Dataset	See Test Setup
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	• The transport layer is tested based on appropriate type of access methodology following RFC 2544 test parameters. • During service implementation and activation stage, the Customer Care manager in conjunction with the customer and the account team we will do a series of tests that include the testing for validation of service features.

Figure 5.4.2.8.8-2. TEST CASE-VTS-Av

Requirement	Description
Parameters Measured	Availability (%)
Measurement Procedure	Percentage of the total reporting interval time that VTS is operationally available to the agency

Requirement	Description
	$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
Acceptance Criteria	Routine Service Level ≥ 99.5%

Figure 5.4.2.8.8-3. TEST CASE-VTS-GOS

Requirement	Description
Parameters Measured	Video conferences that are reserved and confirmed. It shall be calculated as the ratio of the number of locations successfully completing a VTS call divided by the total number of locations scheduling a VTS call within a calendar month. The contractor shall compute the number of completed service requests by counting the cumulative number of locations associated with each conference that were successfully completed.
Measurement Procedure	The contractor shall compute the number of service requests denied by: counting the cumulative number of locations associated with each VTS conference that could not be scheduled for a particular date and time requested in a calendar month. VTS calls that were disconnected and then re-established only due to the fault of the contractor would be included as a denied request.
Acceptance Criteria	More than or equal to 95% VTS conference requests met

Figure 5.4.2.8.8-4. TEST CASE-VTS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.4.2.8.9 DHS Intrusion Prevention Security Service [C.2.8.9.4]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.8.10 Software Defined Wide Area Network Service (SDWANS) [C.2.8.10]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified

for this service in a Task Order. SDWANS underlay services (e.g. BIS, IPS, VPNS and ETS services) will be tested according to the test plans defined for the applicable underlay transport service.

5.4.2.9 Service Related Equipment [C.2.9]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.10 Service Related Labor [C.2.10]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.11 Cable and Wiring [C.2.11]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.2.12 Access Arrangements [C.2.12]

No performance metrics are specified for this service at the IDIQ level. A service verification test plan could be developed based on the specific requirements identified for this service in a Task Order.

5.4.3 Test Scenario TS-03 [C.2.1.6.1.4]

Objective	Verification Testing of Dark Fiber Services
Approach	Lumen's approach is based on the test scenario for each service offered under the EIS contract as identified in this section 5.4.3.
Acceptance Criteria	See Section C.2.1.6.4 for acceptance criteria

5.4.3.1 Dark Fiber Services [C.2.1.6.4]

Figure 5.4.3-1. TS-02-DFS

Requirement	Description

Requirement	Description
Verification & Acceptance Testing Approach	Agencies will acquire dark fiber and have the option of either providing their own opto- electronics equipment or leasing opto-electronics equipment from the contractor. If agencies choose to provide their own opto-electronics equipment, Dark F ber Services provides them with the flexibility of not only designing their optical networks to meet their unique mission requirements but also of owning and managing them so that network infrastructure can be readily modified as needed. If agencies choose to acquire opto-electronics equipment from the contractor, Dark F ber Services provides them with the flex bility of contracting services from the contractor. Lumen will complete test cases as identified in Figures 5.4.2.1.6-2 through 5.4.2.1.6-6 for the DFS verification and acceptance testing.
Test Dataset	See Test Setup.
Fallback Approach	Any service that fails to meet the specified service requirements during acceptance testing or that fails independent Government verification is re-tested at no additional cost to the Government. Lumen will trouble shoot the issues causing the failed test before retesting the service.
Test Setup	The end-to-end attenuation tests and optical time domain reflectometer (OTDR) test shall be conducted for each fiber and a report will be delivered. OTDR testing will ensure that the installed f ber is in good condition and is acceptable for commissioning of electronics. OTDR testing will also aid in fault location, restoration, and maintenance, and DWDM system turn-up OTDR bi-directional testing will be done for each fiber in each span. Any single reflectance event in the OTDR trace will be less than 40 decibels (dB) The Lumen Team will set the OTDR for proper operation in accordance with the length of the f ber span and distance between splices by setting the appropriate pulse width, range, resolution, and averaging time, as specified in the Lumen Team OTDR Set Up Procedures. The Lumen Team will set in the OTDR the proper Index of Refraction and Backscattering Coefficient, matching the f ber's specifications. All connectors will be cleaned with a Chem-Wipe and alcohol or a dry connector cleaner. OTDR settings will remain constant during the testing of all fibers on a span. There will be no smoothing allowed on any traces. The Lumen Team will assume the responsibility of obtaining an acceptable launch on all traces. The Lumen Team will confirm that all field splices of the tested link are identifiable and reported. The Lumen Team will enter into the OTDR the specific location and identification data for the link including end locations and fiber trace. SMF-28 fiber will be tested at 1310 nm. The Corning LEAF f ber will be tested at 1550 nm. The OTDR test will then be conducted in the opposite direction. The OTDR trace data for each direction will be stored onto a CD. Power meter tests ensure that the fiber installed meets compliance and that the signal transmitted through the fiber will remain strong and accurate. Power meter tests aid in the commissioning of transmission electronics. Prior to power meter testing, the Lumen Team will calculate the loss budget. Power meter loss due to all impairments will be less than 0.25 dB/km when measured at a wavelength of 1550 nm for each f ber on each span tested. For Corning LEAF fiber, the Lumen Team will perform the end-to-end power meter test using a stable laser light source at 1550 nm and 1310 nm. The link-loss test on each fiber in the link will be conducted in both directions, at both wavelengths. Lumen Team personnel will ensure that the link connectors and test patch cord

Requirement	Description
	connectors are kept clean at all times during the tests. The connector style used will be SC-UPC and will match connectors within the OSX or FDP shelf. Two fiber patch cords, also with SC UPC connectors, will be used by the Lumen Team personnel throughout the tests to produce a stable reference launch power on the source patch cord and a stable reference loss on the meter patch cord. Lumen Team personnel will document these power and loss data in the Link Loss Report. The Fiber Test Result Submittal Package will be completely filled out by the Lumen Team and submitted within 14 days of test completion. The Lumen Team will maintain all documentation including daily logs, redlines, production figures, fiber forms, test forms, and all electronic media. This documentation will be available to the Government for review. The Lumen Team will provide a final sign-off sheet with all documentation and test results for each specific span that is tested.

Figure 5.4.3-2. TEST CASE-DFS-AC

Requirement	Description	
Parameters Measured	Attenuation Coefficient (AC) SMF (1550 nm) AC SMF (1310 nm) AC MMF 850 nm (50/125 µm) AC MMF 1300 nm (50/125 µm) Attenuation coefficient is the attenuation per unit length with a maximum value at one or more wavelengths. In this case, wavelengths are from 1310 and 1550nm.	
Measurement Procedure	The method used to test the attenuation coefficient of single-mode optical fiber (SMF) is based on bidirectional backscattering measurements. For campus applications, MMF may be used and the attenuation coefficient per unit length is included for 850nm and 1300nm. The values listed in Section C.2.1.6.4 reflect fiber only. Additional allowances will be made for splices and connectors.	
Acceptance Criteria	Attenuation Coefficient (AC) SMF (1550 nm) Routine Service Level ≤ 0.25 dB/km at all times AC SMF (1310 nm) Routine Service Level ≤ 0.35 dB/km at all times	AC MMF 850 nm (50/125 µm) Routine Service Level ≤ 2.35 dB/km at all times AC MMF 1300 nm (50/125 µm) Routine Service Level ≤ 0.35 dB/km at all times

Figure 5.4.3-3. TEST CASE-DFS-PMD

Requirement	Description
Parameters Measured	• Polarization Mode Dispersion (PMD) at 1550 nm (Inter-City Networks) • PMD (Intra-City Networks)
Measurement Procedure	Polarization Mode Dispersion is the term that describes the relationship between polarization and group delay. PMD can limit the highest bit rate that is achievable in a fiber optic system. The

Requirement	Description
	following are the most popular methods of measuring PMD: Fixed Analyzer (also called wavelength scanning), Interferometry, Pointcare arc (also called SOP), Modulation phase shift, Pulse delay, and Baseband Curve fit. The major differences in testing setups among these methods are the type of light source, means of defining spectral width, and means of tuning the wavelength. Measurement data is collected while sweeping or stepping the wavelength of the source (or receiver, depending on the method used). PMD values are to be taken uni-directionally at 1550 nm and analyzed via a route mean square (rms) algorithm for optical spans made up of more than one all-optical and separately tested section.
Acceptance Criteria	May be specified in Task Order

Figure 5.4.3-4. TEST CASE-DFS-CD

Requirement	Description
Parameters Measured	Chromatic Dispersion at 1550 nm
Measurement Procedure	Chromatic dispersion measurements characterize how the velocity of propagation in fiber or components changes with wavelength. This measurement is obtained by analyzing the group delay through the fiber as a function of wavelength. A wavelength tunable optical source is intensity modulated and the phase of the detected modulation signal is compared to that of the transmitted modulation. The wavelength of the tunable source is then incremented and the phase comparison is made again. Calculating how the difference between the two measurements, the group delay is measured.
Acceptance Criteria	May be specified in Task Order

Figure 5.4.3-5. TEST CASE-DFS-RE

Requirement	Description
Parameters Measured	Reflectance Events (all events)
Measurement Procedure	Reflection measurements are done using an optical time-domain reflectometer (OTDR). The OTDR injects a pulsed signal into the optical fiber and a small amount of the injected signal is reflected back (Raleigh Backscattering). By measuring the amount of backscattered signal in relation to time, signal loss in relation to fiber optic cable distance is determined. OTDR measurements are to be taken bi-directionally at required frequencies to properly characterize splice/connector loss, reflectance, attenuation, and fiber length for all transmission bands.
Acceptance Criteria	Routine Service Level ≤ 40 dB at all times

Figure 5.4.3-6. TEST CASE-DFS-TTR

Requirement	Description
Parameters Measured	Time to restore service on a per-incident basis.
Measurement Procedure	Not Applicable. Response times can only be tested upon service activation.
Acceptance Criteria	Without Dispatch: Less than 4 hours With Dispatch: Less than 8 hours

5.5 Test Data Sets [E.2.2.4]

The Lumen Team will successfully test all of the test cases defined in the EIS Test Plan using the appropriate test data sets proposed by Lumen. The Lumen Team will use the appropriate test data sets that reflect real-world service conditions and locations and will address all relevant test cases for the services proposed by Lumen.

6.0 CLIMATE RISK MANAGEMENT PLAN [L.30.2.5, M.2.2, F.2.1 (84-86), G.12]

Purpose

The purpose of this plan is to provide guidance to Lumen personnel supporting Task Orders (TO) under the EIS contract to comply with relevant regulations and executive orders pertaining to Climate Risk Management. Additionally, this plan provides GSA and agency personnel with an understanding of Lumen's approach and commitment to Climate Risk Management.

Lumen Cares: Commitment to Resiliency and Environmental Responsibility

- Global, company-wide focus on sustainability
- Proactive mitigation of climate change risk
- Demonstrated success in reducing environmental impacts
- Annual reporting to Carbon Disclosure Project

6.1 Introduction and Overview [G.12]

This Climate Risk Management Plan supports the following objectives:

- Demonstrate compliance with Federal regulations and Executive Orders
- Align with GSA's climate change adaptation and sustainability plans and initiatives
- Mitigate risks of loss of assets supporting customers under the EIS contract
- Establish continuity strategies to minimize impacts to EIS agency customers
- Demonstrate leadership and innovation in corporate responsibility as a partner of GSA and EIS customer agencies

This Plan applies to all services Lumen provides to EIS customers worldwide.

6.2 Climate Change Adaptation [G.12.1]

Lumen's vision is to be "The Trusted Connection to the Networked World". The strategy that supports this vision includes continuing to expand the scale of our network, building the most efficient and reliable communications platform, and constantly innovating to improve our business.

Lumen Cares

- Compared with 3,400 other companies who submitted 2013 supply chain information to the Carbon Disclosure Project, Lumen received a B grade for our climate change mitigation while the average score was a C.
- In 2015 Lumen was named to the CDP S&P 500 Leaders List.

Lumen was named to 2015 CDP S&P 500 Leaders List. Carbon Disclosure Project (CDP) is an international, not-for-profit organization providing the only global system for companies and cities to measure, disclose, manage and share vital environmental information. This report tracks how the world's largest companies are responding to climate change and highlights companies taking action.

For EIS, particularly in the long term, this strategy is in part influenced by certain consequences of climate change such as increased risks of flood or other catastrophic climate events, as well as rising energy, fuel, and material costs.

6.2.1 Reporting [G.12.1, E.O. 13693]

Lumen will provide sources of publicly available information regarding Lumen-wide environmental impacts and sustainable management practices on Lumen's EIS webpage

Lumen is an active participant in the CDP. Annually, we respond to the Climate Change and Supply Chain questionnaires, providing information on our sustainability initiatives and progress during the previous year. Our responses are publicly available on the CDP.net website. We believe this level of transparency benefits our customers, demonstrates our commitment to corporate social responsibility and accountability, and contributes information that is valuable to the telecommunications industry.

All Lumen sustainability disclosures and reporting are be kept up-to-date and accurate and will be made available for agency use to directly support the Agency Adaptation Plans of agencies procuring services through the EIS contract. Lumen understands that sustainability-related standards, including estimates of the lifecycle costs and environmental impacts of proposed solutions, will apply at the Task Order level.

6.2.2 Climate Change Adaptation in Design and Operations of Services

Climate change adaptations will be considered in the design and operations of services provided under this contract. Lumen's strategy supports our Federal agency customers' efforts to reduce carbon emissions through dematerialization, virtualization,

e-commerce, and smart grid technologies. It also demonstrates our commitment to mitigate the environmental impact of our own operations. We took steps to improve our processes for identifying our risks related to climate change, evaluating improvement opportunities, taking action to mitigate our environmental impacts, and communicating our progress to stakeholder groups.

We built the Lumen network with resilience in mind, using physical plant components and redundant systems to support continuous, uninterrupted services for our customers. Hardware, however, is only part of the solution. Advance planning to develop and rehearse strategies that capitalize on all of our capabilities and enable us to recover our services quickly remains essential. A cross-functional business continuity planning structure spans all regions of the company, adhering to the business continuity policy and framework. As a result, Lumen delivers uninterrupted service and gives our customers confidence that our services will run with minimal interruptions, regardless of the effects of climate change.

6.2.3 Incorporating Climate Change Adaptation in Risk Management Plan

Lumen's climate risk management plan incorporates climate change adaptation strategies into risk management programs to reduce property, infrastructure, and supply chain vulnerabilities. **Figure 6.2.3-1** depicts the Lumen Business Continuity Planning Risk Management Lifecycle.

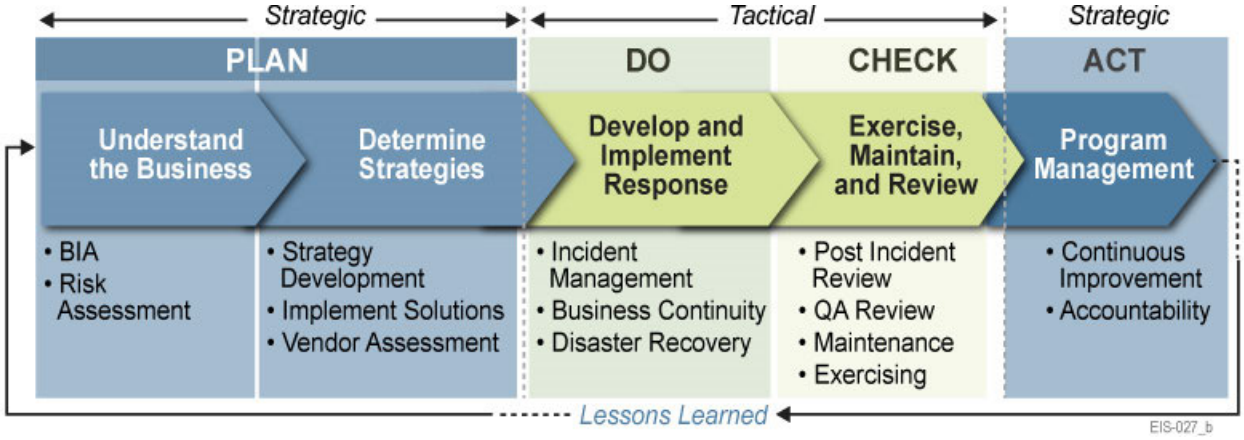


Figure 6.2.3-1. Business Continuity Planning – Risk Management Lifecycle.
Lumen's Risk Management Process supports Climate Change Adaptation.

Our Lifecycle phases are tightly integrated with our overall program management approach and follow the familiar Plan-Do-Check-Act cycle, described in **Figure 6.2.3-2**.

Figure 6.2.3-2. Risk Management Approach.

PHASE	DESCRIPTION
Plan	• Perform business impact assessment • Perform risk assessment • Design and implement continuity strategies
Do	• Develop and activate incident management response structure • Develop and activate business continuity plans • Develop and activate disaster recovery plans
Check	• Exercise, maintain, and train • Capture and promulgate lessons learned
Act	• Revise plan • Implement continuous improvement

The Lumen Corporate Business Continuity Team has overall responsibility for governance of the risk management process. Stakeholders contributing to risk analysis and mitigation planning include the Chief Technology Officer, regional presidents, and the Program Management Offices (PMO) of major customer programs. The EIS Program Manager, Mr. Matthew Scelza, represents the interests of our EIS agency customers in this process.

6.2.4 Planning for Climate Change Related Risk

Lumen's risk planning prepares for a wide range of events, both natural and manmade. The climate-change-related risks we incorporate in our plan include:

- Flooding from rising ocean levels or increased severe weather
- Tornadoes, cyclones, tsunamis, hurricanes and other extreme weather events
- Wildfires
- Civil unrest related to these events

For each risk type, we plan for scenarios involving loss or impacts to business functions, facilities, systems, personnel, and our supply chain. Although some risks have a greater likelihood of occurrence in certain regions or locations, we require all

Lumen facilities worldwide to plan, prepare, and exercise for all risks, ensuring a consistent and effective response in the event of an emergency.

6.2.4.1 Assessing Climate Change Risk [G.12.1]

Lumen's corporate Business Continuity Lifecycle incorporates annually conducting a Business Impact Analysis to understand our most critical functions, facilities, and systems. A risk assessment is used to identify the threats and hazards most likely to impact those critical functions and assets, with the identified risk of disruption then mitigated.

Business Continuity Planning — Scenarios

- Loss of Power
- Loss of Facility
- Loss of Key Employees
- Loss of Network or Segment
- Loss of Critical IT Apps
- Loss of Critical Vendors
- Loss of Critical Equipment

Lumen's corporate Business Continuity Planning framework incorporates development of plans to mitigate the impacts of any scenario including climate change impacts. The hazards/threats that are possible outcomes of climate change include: flooding from rising ocean levels or increased severe weather; disruption to our supply chain; loss of people or facilities due to disruptive natural phenomena such as tornadoes, cyclones, tsunamis, hurricanes, and other extreme weather events; as well as wild fires and civil unrest related to these events. The overall business continuity strategy, processes, and results are communicated to the Regional Presidents and our Chief Technology Officer quarterly.

Figure 6.2.4.1-1 shows the matrix we use to facilitate risk assessment and analysis. First, we identify threats and hazards at a regional and country level. We project their associated probability of occurrence and severity if they do occur, rating them on a scale from (1) Low to (5) High. We then multiply the probability by the severity to arrive at a numerical risk score, which enables us to prioritize the risks.

Figure 6.2.4.1-1. Vulnerability Assessment

	RISK ASSESSMENT	LUMEN EXPOSURE	AREAS IMPACTED BY THREAT/HAZARD

Threat or Hazard	Probability	Severity	Risk Score	Past 12 Months	Network Products/ Services	Power/ HVAC	IT Systems/ Data	People
Windstorm, cyclone, hurricane, tornado, water spout, dust storm or sandstorm								
Fire – Internal (explosion, accident, etc.)								
Flooding – External / water control structure/dam/ levee failure								
Tsunami								
Supply chain delays or disruptions								
Utilities – Communications systems interruptions (external, cellular, PSTN, undersea cable)								
Utilities – Communications systems interruptions (internal, fiber cut, equipment failure)								
Utilities – Electricity								
Utilities – Water								
Utilities – Sewage								
Financial issues, economic depression, inflation, financial system collapse								
Gas leak								
Snow, ice, hail, sleet, avalanche								
Personnel availability								
Landslide, mudslide, subsidence glacier, iceberg								
Extreme temperatures (heat/cold)								
Volcano								
Fuel/resource shortage								
Pandemic/Epidemic								
Fire – External (forest,								

	RISK ASSESSMENT			LUMEN EXPOSURE	AREAS IMPACTED BY THREAT/HAZARD			
Threat or Hazard	Probability	Severity	Risk Score	Past 12 Months	Network Products/ Services	Power/ HVAC	IT Systems/ Data	People
range, urban, wildland, urban interface)								
Lightning strikes								

After prioritizing risk, we conduct an analysis for each impact to determine what has already been done to mitigate it, to determine the overall "residual risk" score using the matrix shown in **Figure 6.2.4.1-2**.

Figure 6.2.4.1-2. Residual Risk Calculation

IMPACTS CAUSED BY ANY THREAT OR HAZARD	PROBABILITY (FREQUENCY OF OCCURRENCE)	SEVERITY (HOW BAD COULD IT GET)	INHERENT RISK	CURRENT LEVEL OF RESILIENCY/ REDUNDANCY	MITIGATED SEVERITY LEVEL	RESIDUAL RISK
Loss of Facility						
Loss of Power/Cooling						
Loss of Key Personnel						
Loss of Network						
Loss of Applications/ Systems						
Loss of Essential Vendors						

For any impact assessed to have an unacceptable level of residual risk, we develop an action plan to mitigate it to an acceptable level.

6.2.4.2 Mitigation Strategies [E.O. 13693]

Resilient Network. Lumen's network is built to be resilient. Diversity, redundancy, and mirroring enable us to provide service continuity to customers affected by climate events. Our global reach on six continents provides alternate routes, access

to alternate carriers, alternate Network Operations Centers (NOC) (mirrored, with automatic failover), and alternate storage and spares sites.

Lumen has a demonstrated ability to restore service after a catastrophic event such as Superstorm Sandy. Unlike other carriers in the region, we did not experience flooding in our network facilities. Working with local power companies and the U.S. Army Corps of Engineers, we were able to restore service quickly to our customers. Following the tsunami and nuclear disaster in Fukushima, Japan, Lumen restored two circuits terminating in Yakota, Japan in just two (2) days, enabling our DoD customer to get back up and running. We then restored a third circuit terminating in Misawa, Japan by rerouting it around the disaster zone. In the Middle East, we have restored service in areas affected by Islamic State fighting or other hostilities, by routing through alternate countries and using undersea assets as necessary.

Resilient Supply Chain. Recognizing the importance of our suppliers and vendors in enabling us to support our customers, Lumen incorporates risk planning into our supply chain relationships. We evaluate each supplier's resiliency and work with them to develop an action plan. We also include suppliers in exercises of our own action plans. Contracts include business continuity service level agreements that may involve use of alternative transportation methods, or delivery to one of our geographically dispersed spares depots, managed by UPS – one in every major market.

We also maintain an active roster of alternate suppliers and carriers around the world. This has proven especially important with OCONUS, where host nation permits may be required. In supporting a DoD customer in the Middle East, we were able to quickly mobilize a regional support vendor in the Middle East when the host nation denied base access to our primary vendor. Our mutual agreements with international and regional telecommunications carriers provide rapid rerouting capabilities to supplement our own extensive network.

6.2.4.3 Testing and Revision

Our worldwide Lumen facilities test our mitigation strategies annually. These tests include tabletop exercises, which take the form of a group discussion of a hypothetical scenario, and operational exercises, which are live, real-time simulations of real-world scenarios. Following each exercise, we capture lessons learned and evaluate what worked and what needs improvement. We use this analysis to develop and implement an after-action plan. If the exercise did not meet all objectives, we revise relevant aspects of the mitigation strategy and provide training to our personnel on the revised strategy.

6.2.5 Reporting and Regulatory Compliance [F.2.1 (84-85), G.12.1, E.O. 13693]

Lumen's management systems and written policies enforce compliance with laws, rules, and regulations that are applicable to our business in all countries in which we operate. These include Executive Orders 13693, as applicable to EIS. Our EIS Contractor Program Management Office (CPMO) will notify the agency and the GSA CO immediately if conditions arise thought to be non-compliance with the applicable Executive Order.

In accordance with EIS contract requirements, we submit to GSA an annual EIS Climate Change Adaptation, Sustainability, and Green Initiatives Report (deliverable EIS RFP Section F.2.1 (85)) that reflects our progress during the previous year. As previously noted Lumen uses accredited third parties like CDP for corporate sustainability reporting.

Additionally, we revise this Climate Change Risk Management Plan (deliverable EIS RFP Section F.2.1 (84)) as needed to accommodate new regulatory requirements, newly identified climate risks, and new mitigation strategies.

6.3 Sustainability and Green Initiatives [G.12.2, E.O. 13693]

6.3.1 Sustainable Products

Lumen will provide sustainable products and services whenever possible under the EIS contract. Lumen will comply with EIS RFP Section G.12.2 and provide products

and Information and Communications Equipment (ICT) equipment that is sustainable and energy efficient to the greatest extent possible. It should be noted that Energy Star and EPEAT program compliance generally applies to IT equipment vs. ICT equipment. None of the current Lumen suppliers of ICT equipment are participating manufacturers in the EPEAT program.

If Lumen opts to offer Energy Star-certified, low standby power, or EPEAT-registered products then we will identify by model which products offered are Energy Star-qualified/certified, meet FEMP low standby power levels, and/or EPEAT-registered, with EPEAT-registered products broken out by registration level of bronze, silver, or gold.

6.3.2 Sustainability in Design and Operations of Services

Both the sustainable acquisition and data center requirements of Executive Order 13693 – Planning for Federal Sustainability in the Next Decade will be considered in the design and operations of Lumen services to be provided under this contract. The leadership and employees of Lumen are committed to always doing the right thing, demonstrating good corporate citizenship in the communities in which we operate, including being good stewards of the environment. In 2013, we launched Lumen Cares, our global Corporate Social Responsibility (CSR) program, consisting of initiatives built around employee volunteerism, charitable giving, and our environmental sustainability program.

At Lumen, environmental sustainability is managed by a cross-functional team that includes Corporate Health Safety & Environment, Utility and Energy Management, Supply Chain Management, Real Estate, Field Services/Environmental Management, and Lumen Cares. This team periodically evaluates the environmental impact of the company's operations and collaborates with stakeholder groups to identify, evaluate, and help implement innovative strategies, technologies, process improvements, or other solutions to mitigate these impacts.

Each of our operating regions in North America, Europe Middle East Africa (EMEA) and Latin America (LatAm) establishes annual environmental sustainability targets. In some countries in EMEA and LatAm, we manage our environmental impacts through formal Environmental Management Systems that are accredited in accordance with ISO-14001 requirements. We communicate our annual results to all employees through our company intranet ("Next Level") and our climate change/greenhouse gas (GHG) emission reduction activities are publically reported to the Carbon Disclosure Project (CDP), with those reports available to registered CDP users.

Lumen Cares
Lumen obtained ISO-14001 registration for our Environmental Management Systems in Latin America.

Environmental sustainability is a priority at every level of the organization. To encourage continuous improvement and sustained commitment to environmental sustainability goals, we have incorporated environmental performance into our incentive programs (**Figure 6.3.2-1**) to recognize employees for their contributions toward greater energy efficiency and reduced GHG emissions.

Figure 6.3.2-1. Lumen Sustainability Program Incentives

CONTRIBUTOR	AWARD	DESCRIPTION
Energy managers	Monetary reward	Energy managers are incentivized to meet overall energy consumption reduction and energy efficiency performance indicators by linking achievement of these indicators with the employees' annual performance review/rating and incentive bonus award. Achieving established targets for energy consumption and efficiency contribute to reducing the company's carbon emissions/intensity and influencing energy manager's overall compensation.
Facility managers	Monetary reward	Facility managers are responsible to meet site-specific energy consumption and efficiency performance indicators typically based on Power Usage Effectiveness (PUE). Achieving these performance indicators are part of the Facility Managers' annual performance evaluation/rating and incentive bonus award. Achieving established facility targets for energy consumption and efficiency contribute to reducing the company's carbon emissions/intensity and influencing designated facility manager's overall compensation.
Environment/ Sustainability managers	Monetary reward	Environmental/Sustainability managers are responsible to meet established functional targets including reduction of overall carbon emissions and/or intensity. Achieving these performance indicators are part of annual performance evaluation/rating and incentive bonus awards. Achieving environmental sustainability targets related to energy and materials reduction, re-use, and recycling contr bute to reducing the company's carbon

CONTRIBUTOR	AWARD	DESCRIPTION
		emissions/intensity and influencing environment/sustainability manager's overall compensation.
Field Operations employees	Recognition (certificate and gift)	Employees are recognized for identifying and helping to implement effective energy efficiency ideas. This program is known as "Reduce the Juice" and the energy efficiency measures help reduce our overall carbon emissions/intensity. Employees who submit the most impactful ideas are presented with an award certificate and gift card and recognized in company internal communication from their Senior Vice President.

Our significant environmental focuses and [illegible] address them, as well as the results of these initiativ[illegible] paragraphs.

2014 Energy Efficiency Project Results

- Avoiding 29,000 metric tons of greenhouse gas emissions
- Saving over 25,000 MWH of electricity
- Helping reduce the incidence of health problems related to particulates and other air pollutants

6.3.2.1 Greenhouse Gas Emissions – Energy Use

As a global facilities-based telecommunications provider, our most significant environmental aspect is energy use, particularly the purchase of electricity resulting in greenhouse gas (GHG) emissions. Lumen mitigates this impact by monitoring and managing facility energy consumption and associated utility costs. Lumen initiatives such as enhanced building and energy management systems, facility system optimization, operational best practices, utility metrics reporting, renewable energy contracts, and energy awareness programs optimize network facility operation and improve energy efficiency.

For example, in 2014 we implemented 80 energy-related projects that resulted in avoiding nearly 29,000 metric tons of carbon emissions compared to business-as-usual. As a result of these projects and other factors, Lumen reduced our year-over-year global GHG emissions by 4 percent. In addition to facility energy use, Lumen is proactively managing other carbon-emitting activities such as fleet vehicle use and employee transportation and travel.

Lumen is currently on track to achieve our energy efficiency and GHG emissions reduction targets for 2015. Those targets are summarized below in **Figure 6.3.2.1-1**.

Figure 6.3.2.1-1. Lumen 2015 Emission Reduction Targets

REGION	2015 GHG EMISSIONS REDUCTION TARGETS
North America	Reduce energy by 16,000 MWh and GHG emissions by 8,660 MTs at targeted facilities
EMEA	Reduce GHG emissions by 2% compared to 2014
LatAm	Establish a GHG reduction plan compared to 2014 baseline data

6.3.2.2 Fleet Operations

In the past several years, Lumen has significantly improved the fuel efficiency and overall performance of the fleet vehicles used by our Field Operations team to maintain our communications network. Since 2010, we have increased fuel efficiency of our North American fleet vehicles by approximately 12%, thereby avoiding over 2,400 lbs of GHG emissions per year for each vehicle in our fleet. Reducing our per-vehicle effect on global climate change was achieved by:

- Investing in newer and more fuel-efficient vehicles
- Leveraging process improvement and our GPS-based Fleet Management System to more efficiently use our fleet vehicles
- Training field technicians in techniques to avoid vehicle collisions, improve fuel efficiency, and reduce maintenance and repair costs

6.3.2.3 Employee Transportation and Travel

Lumen has established a transportation pre-tax payroll deduction program to benefit our employees who use public transportation or other allowable expenses during their commute to work. This program helps to decrease greenhouse gas and other air emissions.

Lumen's travel policy encourages employees to minimize travel, thus reducing the impact of company activities on the environment. To reduce the need for travel, we have made significant investments in technologies to facilitate group communications among employees, customers, and business partners. Lumen also allows telecommuting for employees with manager approval, which reduces employee commuting and decreases our environmental impact.

Our employees are committed to reducing their personal environmental footprint. At our headquarters offices in Broomfield, CO, we provide seven electric car-charging

stations (four ports with reporting functionality) for employee use. Since inception in 2013, this program has yielded the following results:

- Charging sessions – 2,751
- Carbon emissions avoided – 9,483 kilograms
- Gasoline saved – 2,833 gallons

6.3.2.4 Waste Management and Reduction

Lumen's waste management and reduction program mitigates environmental impacts through source reduction/re-use and recycling.

6.3.2.4.1 Source Reduction/Reuse

Source reduction reduces or eliminates the generation of waste at the source and reduces the use of hazardous materials in production. We achieve source reduction/ reuse through redeploying equipment to extend its useful lifespan, selling end-of-life equipment on the secondary market, and avoiding the generation or procurement of unnecessary items. For example, expanding our paperless billing programs, using double sided printing as a default printer setting, and removing Lumen from sources of junk mail, we avoid waste that results in the a variety of environmental benefits.

Figure 6.3.2.4.2-1. Lumen Recycling Programs. *Lumen Recycling Programs are comprehensive and support Federal/GSA Sustainability and Green Initiatives.*

6.3.2.4.2 Reuse/Recycling

Our recycling programs include the reuse or recovery of in-process materials or materials generated as byproducts that

can be processed further onsite or sent offsite to reclaim value (**Figure 6.3.2.4.2-1**). Lumen has implemented recycling programs to achieve our corporate social responsibility objectives, maintain regulatory compliance, and mitigate environmental impacts. These efforts have included:

- Recycling 1,375 tons of end-of-life batteries, thereby preventing an estimated 920 tons of lead and 138 tons of sulfuric acid from entering the environment
- Recycling 167 tons of company owned electronic waste such as computers, monitors, laptops, printers, mobile phones, and servers that require special handing due to the presence of regulated hazardous chemicals. Recycling these waste electronics resulted in avoiding:
  - 881 tons of GHG emissions (equivalent to eliminating 537 cars from the road for 1 year)
  - 56,470 tons of air emissions and 32,048 gallons of water consumption
  - Energy use equivalent to that required by 1,236 homes for 1 year
  - Generating a volume of hazardous waste equivalent to the weight of 13,517 bricks
  - Recycling/composting 92 tons of office waste at our Broomfield, CO headquarters; thereby preventing:
    - 2,609 pounds of air pollution
    - Energy use equivalent to that required by 22 homes for one (1) year
    - 304,305 gallons of water and 7,175 gallons of gasoline
    - 139 cubic yards of landfill space and 739 trees

6.3.3 Compliance with Climate Change Adaptation Conditions

Lumen will comply with the climate change adaptation conditions described in the aforementioned EO and other applicable laws, regulations, and directives.

6.3.3.1 Notification of Non Compliance

Lumen will notify the agency and GSA COR immediately if conditions arise thought to be out of compliance with aforementioned EO and other applicable laws, regulations, and directives.

6.3.3.2 Applicable Products Covered Under Federal Energy Programs

Lumen will comply with EIS RFP Section G.12.2 and provide products and Information and Communications Equipment (ICT) equipment that is sustainable and energy efficient to the greatest extent possible. It should be noted that Energy Star and EPEAT program compliance generally applies to IT equipment vs. ICT equipment. None of the current Lumen suppliers of ICT equipment are participating manufacturers in the EPEAT program.

6.3.3.3 Data Centers Meeting Power Efficiency Targets

Lumen's data centers and cloud services power utilization efficiencies are covered in Section 6.3.5 of this plan.

6.3.4 EPEAT and Energy Star [G.12.2.1, G.12.2.2, E.O. 13423]

Under this contract, Lumen will deliver, furnish for government use, or furnish for contractor use at a federally-controlled facility, commercially available equipment that was EPEAT bronze-registered at the bronze level or higher throughout the life of the contract. In procuring equipment for Lumen service-providing facilities, we seek products that support our energy-efficiency and air emissions reduction objectives.

In accordance with EIS contract requirements, we submit to GSA an annual EIS Climate Change Adaptation, Sustainability, and Green Initiatives Report (deliverable F.2.1 (85)) that reflects our progress during the previous year. As previously noted Lumen uses accredited third parties like CDP for corporate sustainability reporting.

6.3.5 Data Centers and Cloud Services [F.2.1 (86), G.12.2.3, E.O. 13693]

Lumen currently does not have data centers meeting power utilization efficiencies (PUE) between 1.2 and 1.4 on an annualized basis. Under the EIS contract Lumen will report annually the PUE of data centers used under the EIS contract.

The Lumen Team cloud services are provided through our teammates include their latest datacenter designs, the PUE—a measure of overall building load divided by IT load—average 1.12-1.2 depending on physical location, representing a substantial energy reduction versus the industry average of 1.8.

The Lumen Team will report annually the PUE of data centers used under the EIS contract.

6.4 Deliverables [F.2.1 (84-86), G.12.1]

Lumen will provide the following deliverables for this plan as noted in **Figure 6.4-1**. We will conduct corporate sustainability reports through those accredited third parties designated by the Government and provide copies of the reports to the GSA.

Lumen will collaborate closely with the GSA PMO and EIS customer agencies to ensure that we maintain a current list of deliverables for this plan and review content to ensure compliance with any modifications to the Task Order.

Figure 6.4-1. Climate Risk Management Deliverables

ID	REQUIREMENT REFERENCE	DELIVERABLE DESCRIPTION REFERENCE	DELIVERABLE NAME	FREQUENCY	DELIVER TO
84	G.12.1	G.12.1	Corporate Climate Risk Management Plans	Initial: With proposal Update: As needed	GSA CO, OCO
85	G.12.2.1	G.12.2.1	Climate Change Adaptation, Sustainability, and Green Initiatives Report	Initial: By award Update: Annually from contract award	GSA CO, GSA COR, OCO
86	G.12.2.3	G.12.2.3	Power Utilization Efficiencies (PUE) Report	Initial: Task Order from proposal Update: Annually	OCO

6.5 References [G.12]

This Plan complies with the documents identified in **Figure 6.5-1**.

Figure 6.5-1. References

CATEGORY	RELEVANT DOCUMENTS
Executive Orders	• 13693 Planning for Federal Sustainability in the Next Decade
GSA Plans	• GSA Strategic Sustainability Performance Plan • GSA Climate Change Risk Management Plan

Lumen Policies	• Business Continuity Policy • Lumen Cares Program • Waste Management Guidelines

7.0 FINANCIAL REPORT (SAMPLE) [L.30.2.6, M.2.2, G.9.5, F.2.1 (80)]

Purpose

Lumen will furnish the PMO with a required monthly Financial Status Report that shows the total dollar activity for the month and will be broken down by the service types and services. Our overall approach details are reflected in this attachment.

7.1 Introduction and Overview

Lumen has a long history of complying with GSA's financial management requirements on IDIQ contracts and has the processes and systems in place to comply with EIS program requirements. Lumen will deliver the Financial Management Report and support the Government's contractor requirements for Price Management Mechanism.

Financial Status Highlights

- Accurate totals for direct billing with running totals spent YTD
- History of successfully providing financial status reports to GSA
- Support for GSA PMM process

7.2 Monthly Financial Status Report [G.9.5]

Lumen will provide the Financial Status Report as one of the monthly EIS deliverables. This report will be created by the customer financial service team, with delivery through the Contracts Manager to the GSA EIS PMO. This report will show the total dollar activity for the month, broken down by the service types and services as outlined in Section B of the RFP. This includes:

- The total billed charges for all agencies during the monthly reporting period for direct billing accounts
- The remaining amount of unspent dollars under the maximum contract dollar limitation
- Other totals deemed pertinent to GSA for this contract

As requested, Lumen will update the list of service types and services with new or improved services according to any contract action that deletes services from the list.

7.2.1 Proposed GSA EIS Financial Status Report Format

Contained in **Figure 7.2.1-1** is a sample format of the report Lumen will provide for this contract. It is Lumen's goal to update reporting to meet both GSA and other

agency's reporting needs through the life of the contract. The sample mock-up of the report, as represented in **Figure 7.2.1-1** below in Microsoft Excel, contains the following fields:

- Total Billed Charges for All agencies
- Total Billed Charges for All Direct Billed agencies
- Remaining Obligation under the Minimum Revenue Guarantee
- Remaining Amount of Unspent Dollars Under the Maximum Contract Dollar Limitation
- Total Billed Charges to be Reconciled

7.2.2 Proven Financial Reporting Performance on GSA's current contract vehicles

Lumen, as a GSA contract holder under Networx, WITS 3, GRITS and Schedule 70, provides monthly financial status reports that are both timely and accurate. **Figure 7.2.2-1** is an example of the current Networx monthly report and includes the following data:

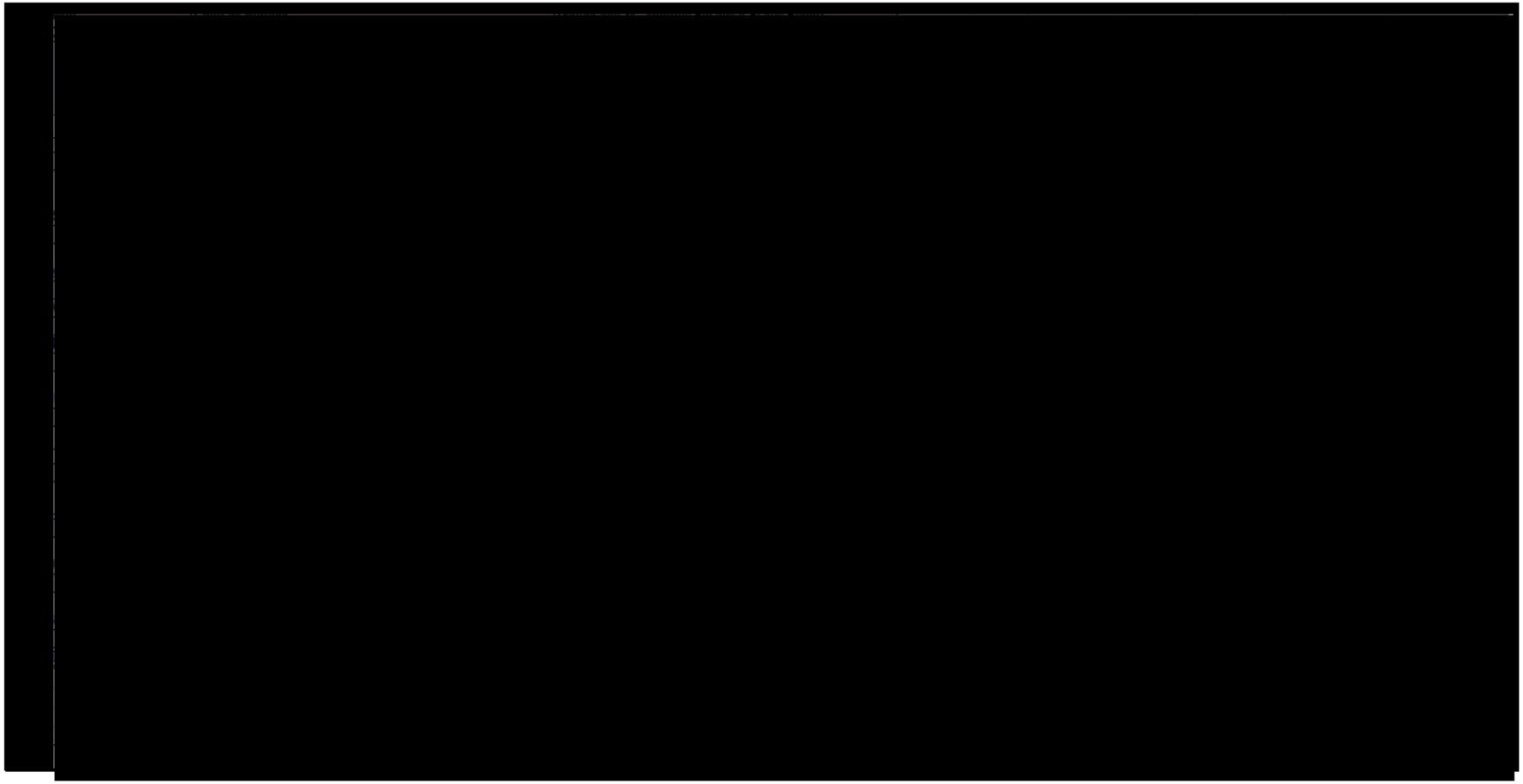
- Invoice number
- AHC number
- Service Type
- Date Submitted
- Invoice amount
- Days outstanding
- Adjustments as applicable
- Total paid
- Total due direct
- Remaining dollar obligation for the minimum revenue
- Remaining unspent maximum revenue

Figure 7.2.1-1. Sample of Lumen's EIS Contract Monthly Report

Contractor: Lumen Technologies	Contract Number: TBD	Deliverable 80 - Monthly Financial Status Report				
Service Type	Service	Total Billed Charges for All Agencies	Remaining Obligation under the Minimum Revenue Guarantee	Remaining Amount of Unspent Dollars Under the Maximum Contract Dollar Limitation	Total Bills Charges to be Reconciled	Remaining MRG
	Virtual Private Network Service					
	Ethernet Transport Service					
	Optical Wavelength Service					
Data Service	Private Line Service					
	Synchronized Optical Network Service					
	Dark Fiber Service					
	Internet Protocol Service					
	Internet Protocol Voice Service					
	Circuit Switched Voice Service					
Voice Service	Toll Free Service					
	Circuit Switched Data Service					
Contact Center	Contact Center Service					
Colocated Hosting Service	Colocated Hosting Service					
	Infrastructure as a Service					
	Platform as a Service					
Cloud	Software as a Service					
	Content Delivery Network Service					
Commercial Satellite	Commercial Mobile Satellite Service					
Communications Service	Commercial Fixed Satellite Service					
	Managed Network Service					
	Web Conferencing Service					
	Unified Communications Service					
	Managed Trusted Internet Protocol Service					
Managed Services	Managed Security Service					
	Managed Mobility Service					
	Audio Conferencing Service					
	Video Teleconferencing Service					
	DHS Intrusion Prevention Security Service					
Access Arrangements	Access Arrangements					
Service Related Equipment	Service Related Equipment					
Service Related Labor	Service Related Labor					
Cable and Wiring	Cable and Wiring					
Total						

EIS-197_DNc

Figure 7.2.2-1. Lumen's Networx Monthly Financial Status Report



7.3 Deliverables [F.2.1 (80)]

Lumen will provide the following deliverables for this plan as noted in **Figure 7.3-1**. We will collaborate with the GSA PMO and EIS customer agencies to ensure that we maintain a current list of deliverables for this plan and review content to ensure compliance with any modifications to the Task Order.

Figure 7.3-1. Financial Management Report Deliverables

ID	REQUIREMENT REFERENCE	DELIVERABLE DESCRIPTION REFERENCE	DELIVERABLE NAME	FREQUENCY	DELIVER TO
80	G.9.5	G.9.5	Financial Status Report	Initial: 30 days after NTP; Update: 15th of each subsequent month	GSA PMO

8.0 BSS RISK MANAGEMENT PLAN [L.30.2.7, M.2.2, G.5.6]

8.1 Introduction [G.5.6]

Lumen's EIS Business Support Systems (BSS) Risk Management Framework Plan addresses system security in accordance with EIS RFP Section G.5.6.

8.2 BSS Risk Management Framework Plan [G.5.6.1, G.5.6.2]

Lumen ensures security requirements are met for the BSS which will be defined in the BSS System Security Plan (BSS SSP), at a Moderate impact level and will support Government security and authorization efforts. Lumen also supports the Government's efforts to verify that these standards are being met. Lumen is committed to maintaining the security, integrity and availability of its services, networks and customer data transported via Lumen services. Lumen operates an integrated security architecture managed by several dedicated security groups. The responsibilities of these security departments are to identify and correct vulnerabilities that affect the commercial and internal netwroks, associated products and services and related support systems. Lumen believes that early detection and analysis of security threats and exposures that impact the network is critical to providing a consistent assessment of the security level being provided. The EIS BSS risk management framework supports the following goals:

- Integration of information security requirements into the service architecture and corresponding system development life cycle
- Implementation of continuous monitoring to support ongoing security authorization decisions
- Implementation of appropriate risk mitigation strategies

In order to develop an effective and relevant security control selection that will ensure that Lumen is able to meet Confidentiality, Integrity and Available objectives in the EIS BSS environment, we have established the BSS Risk Management Framework (RMF) with guidance from the the following documentation:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information security)
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.)
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems." Dated February 2004.
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems." Dated March 2006.
- NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems." Dated February 2006.
- NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments." Dated September 2012.
- NIST SP 800-34 Revision 1, "Contingency Planning Guide for Information Technology Systems." Dated May 2010.
- NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." Dated February 2010.
- NIST SP 800-40 Revision 3, "Guide to Enterprise Patch Management Technologies." Dated July 2013.
- NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems." Dated August 2002.
- NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Dated April 2013.

- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans.” Dated December 2014.
- NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
- NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
- NIST SP 800-160 “Systems Security Engineering.” Draft dated May 2014.
- NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.” Dated April 2015.
- NIST SP 800-171, “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations.” Dated June 2015.
- DODI 8510.01 “Risk Management Framework (RMF) for DOD Information Technology (IT).” Dated 12 March 2014.

The Lumen Security Compliance organization is responsible for the design, maintenance and enforcement of the security framework and other security initiatives within Lumen Communications. The Security Compliance organization is led by the Chief Information Security Officer (CISO). The Security Compliance organization supports the governance of Tier 1 functions described in NIST 800-37.

From the EIS BSS perspective, NIST 800-37 Tier 2 risk management functions are overseen by the Security Architecture and Security Engineering organizations. Security Architecture provides a focus for research and development in identifying, investigating and testing newly discovered security trends, capabilities and technologies. This group is also responsible for the overall security architecture used to protect the Lumen systems and infrastructure. Security Engineering provides a dedicated focus for the development and/or purchase of security technology that

ensures the security and integrity of Lumen's assets and infrastructure as well as the testing and integration of that technology into the logical and physical environement. Additionally, the Lumen Information Technology and Product Development organizations are responsible for information systems associated with a given service and the respective Systems Development Life Cycle (SDLC) management of internally developed systems. The Lumen procurement organization is also integrated into this layer to ensure that risk management constructs are incorporated into the procurement/supply chain.

Within the EIS BSS risk management construct, there are multiple Lumen organizations supporting relative NIST 800-37 Tier 3 support functions. The Network Operations (NOC) and Security Operations (SOC) groups provide 24/7 monitoring and incident management to all operational aspects including security threats. The Network and Security Advanced Services organizations provide Tier III support for the Enterprise, Managed Security Services, Facilities and Lawful process to ensure the availability and reliabiltiy of network and security applications and services within defined SLAs. These organization also ensure that all processes are adhered to in the documentation and implementation of systems. Additionally, Lumen maintains a Security Threat Lab to provide an evaluation and assessment function to the Security Engineering department. The Security Threat Lab is used to regularly review commercial security products. They also perform assessments on the network, systems, applications and functions and test functional aspects of code used within the infrastructure. Protection of service infrastructure extends to the physical security of the service environment. Lumen's Physical security organization develops, designs, deploys and maintains access control and video surveillance systems at Lumen locations worldwide. Following NIST 800-37 guidance, a representative Lumen EIS BSS Tiered Risk Management pyramid diagram is provided in **Figure 8.2-1**.

Figure 8.2-1. Lumen Tiered Risk Management Approach.

RMF plans evolve, and this document summarizes the status of Lumen's plan as of mid-January 2016 for the six RMF steps, recapped in **Figure 8.2-2**. At a high level, we are in Step 2 and will tune it and move to Step 3 as we conclude the Systems Design within our SDLC. To date, we have documented key functional and security requirements (including the SCRM, attached as Section 3 of the Management Volume), and key operational and security requirements within Lumen. Our security organization is engaged, assisting in the first risk analysis and assessment (RA-3), and is maintaining the BSS SSP following the guidance of NISP SP 800-18 Rev.1.

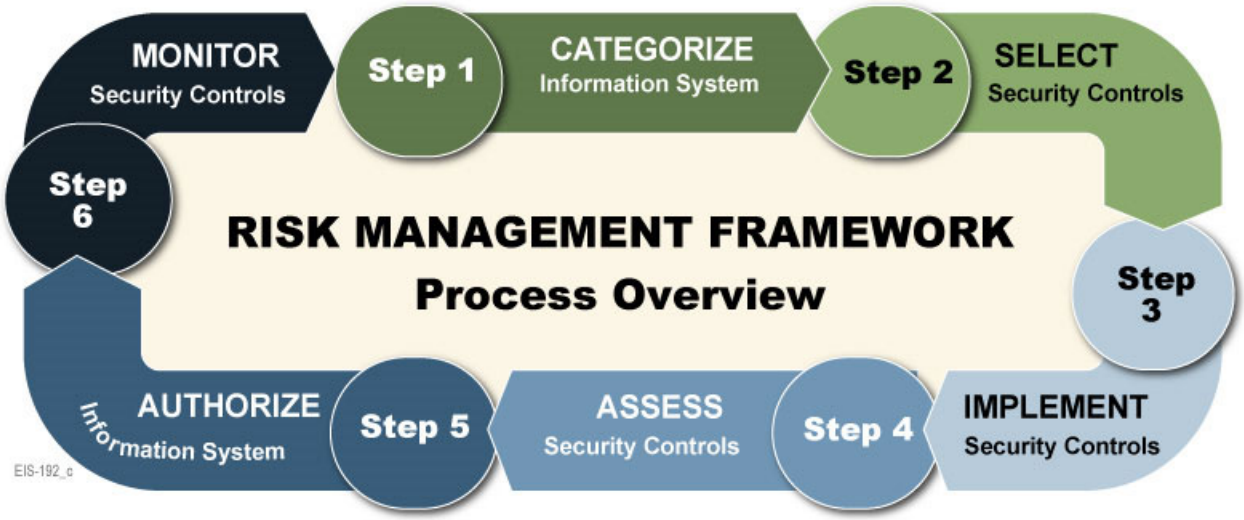


Figure 8.2-2. The Risk Management Framework Cycle.

Addressing each of its six steps, our current RMF follows.

8.2.1 Step 1: Categorize Information System

8.2.1.1 Security Categorization, RMF Task 1-1

Lumen will utilize FIPS 199 for categorization guidance as well as EIS guidance associate with the SBU dataset. Attributes include:

- Data Definition
- Application Regulations, Policies and Standards
- Confidentiality, Availability, Integrity Classifications
- Risk Impact and Threat Analysis

The security categorization of the EIS BSS is given as a MODERATE impact system. Although this conclusion is a given, Lumen has still conducted a risk assessment (RA-3) that is part of this RMF task. Among other items, the risk assessment recognized the information to be processed by the EIS BSS, that this processing may, upon customer request, include decrypting information considered encryption-secured, that all information must be stored, and that, in some cases, personal information could be exposed to the system. The analysis also considered what bounds should be in place to control system access, as well as the consequences of a successful malware attack and exfiltration.

8.2.1.2 Information System (EIS BSS) Description, RMF Task 1-2

The EIS BSS will be built as a separate environment, based upon the existing OSS/BSS supporting Networx Enterprise and WITS 3. EIS specific BSS features and modifications will be added as required. The core system security features of the incumbent systems will be leveraged to meet BSS security requirements. Lumen's current BSS includes strong authentication and is built for high availability, which supports our Disaster Recovery (DR), Business Contingency Planning (BCP), and Continuity of Operations Planning (COOP) program capabilities. For EIS, our BSS solution will support all BSS Component Service Requirements specified in Section G.5.4 of the EIS RFP. These systems interface with our back-end systems to provide

provisioning and operational support through a secure boundary with well-defined interface specifications controlled through a Lumen DMZ and firewall platforms.

The methods, procedures and controls implemented within the BSS security boundary protect government information within the BSS operating envorinment. All EIS related government information is contained within the BSS security boundary. Government information passed to systems outside of the BSS security boundary is obfuscated.

Lumen's GSA Customer Portal is a secure, Internet-accessible Web-based user interface to the BSS that supports ordering, billing, inventory, provisioning, and network management of services procured via the GSA EIS program.

The current portal architecture has been well received by our agency customers and includes robust support for service ordering, operational support, billing, inventory management, trouble handling, training, and customer service. The current GSA Customer Portal delivers real-time program information from operations, trouble ticketing, billing, ordering, and network performance systems.

The services and features inherent in Lumen's GSA Customer Portal are installed, operated, and maintained at Lumen facilities in Broomfield, CO and mirrored at the Lumen Network Operations Center in Atlanta, GA. The proposed EIS BSS environment will be deployed in the same facilities, utilizing common controls developed for the incumbent BSS environment.

The Lumen GSA Customer Portal will be implemented using a service-oriented architecture to directly interface with the EIS BSS through secure Web services. This provides the Government and our operational groups a 24/7/365 real-time view into the EIS BSS redundant data clusters that protect against hardware failures. Our architecture includes dedicated servers to load-balance requests across the Web and application servers, optimizing the application's performance and response time.

The accreditation boundary surrounds hosted and managed servers and their network interfaces into the public internet and the edge of the Lumen network and

provisioning systems. External access to the boundary is controlled by DMZ based firewalls, IDS/IPS. Further logical isolation is provided by separate identity management and access control systems that control access from the trusted to untrusted system boundaries. **Figure 8.2.1.2-1** depicts the components within the Lumen EIS BSS architecture.

Figure 8.2.1.2-1. Lumen's EIS BSS Architecture.
Identifies the EIS boundary infrastructure applicable for the BSS RMF.

8.2.1.3 Information System (BSS) Registration, RMF Task 1-3

The Lumen Security Department system inventory already includes the EIS BSS as the relationships between BSS and governing and operational organizations. This registration process will be updated and maintained as the EIS BSS progresses through its lifecycle.

8.2.2 Step 2: Select Security Controls

8.2.2.1 Common Control Identification, RMF Task 2-1

Lumen is fortunate that many of the controls to be put in place for the EIS BSS are either inherited (i.e., common controls) or heavily derived from controls in place for other systems. The high degree of overlap is apparent as we discuss the controls planned for the EIS BSS in the following section.

8.2.2.2 Security Control Selection, RMF Task 2-2

Based on results of the categorization, NIST 800-53 rev 4 will be used to tailor the security controls to the needed baseline as well as ensure GSA policy alignment. Attributes include:

- Control Tailoring Worksheets
- 800-53 MODERATE baseline controls
- Type of controls – system specific, common, hybrid

As noted, by virtue of its existing security service offerings both commercially and for the Government, its familiarity and comfort in the security environment, and its overall physical and operational infrastructure in place, Lumen is extremely well positioned to design, certify, and operate a designated MODERATE impact level system such as the EIS BSS. As suggested below in the control summary figures, we are approaching the controls for the EIS BSS with a significant head start as almost all of them build upon controls already in place for the GSA Networx Enterprise and WITS 3 programs.

For reference purposes, **Figures 8.2.2.2-1 through 8.2.2.2-19** below are summarize the Control Families and specific controls of the FISMA Moderate impact baseline. Specific controls will be determined as the EIS BSS environment development evolves.

Figure 8.2.2.2-1. Access Control (AC) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AC-1	Access Control Policy and Procedures	AC-1	Access controls establish the terms and conditions under which a person or process can access the system, and the controls placed on such access. EIS BSS access controls will build upon Lumen's stringent access control policies and approval procedures in place for the incumbent GSA WITS 3 and Networx
AC-2	Account Management	AC-2 (1) (2) (3) (4)	
AC-3	Access Enforcement	AC-3	
AC-4	Information Flow Enforcement	AC-4	
AC-5	Separation of Duties	AC-5	
AC-6	Least Privilege	AC-6 (1) (2) (5) (9) (10)	
AC-7	Unsuccessful Logon Attempts	AC-7	

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AC-8	System Use Notification	AC-8	Enterprise BSS environment
AC-11	Session Lock	AC-11 (1)	
AC-12	Session Termination	AC-12	
AC-14	Permitted Actions without Identification or Authentication	AC-14	
AC-17	Remote Access	AC-17 (1) (2) (3) (4)	
AC-18	Wireless Access	AC-18 (1)	
AC-19	Access Control for Mobile Devices	AC-19 (5)	
AC-20	Use of External Information Systems	AC-20 (1) (2)	
AC-21	Information Sharing	AC-21	
AC-22	Publicly Accessible Content	AC-22	

Figure 8.2.2.2-2. Awareness and Training (AT) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AT-1	Security Awareness and Training Policy and Procedures	AT-1	Will be derived from existing Training policies and procedures.
AT-2	Security Awareness Training	AT-2 (2)	
AT-3	Role-Based Security Training	AT-3	
AT-4	Security Training Records	AT-4	

Figure 8.2.2.2-3. Audit and Accountability (AU) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU controls are essential for security-related investigations and Lumen has AU controls in place for other security offerings. EIS BSS will build upon the audit and accountability policies and approval procedures in place.
AU-2	Audit Events	AU-2 (3)	
AU-3	Content of Audit Records	AU-3 (1)	
AU-4	Audit Storage Capacity	AU-4	
AU-5	Response to Audit Processing Failures	AU-5	
AU-6	Audit Review, Analysis, and Reporting	AU-6 (1) (3)	
AU-7	Audit Reduction and Report Generation	AU-7 (1)	
AU-8	Time Stamps	AU-8 (1)	
AU-9	Protection of Audit Information	AU-9 (4)	
AU-11	Audit Record Retention	AU-11	
AU-12	Audit Generation	AU-12	

Figure 8.2.2.2-4. Security Assessment and Authorization (CA) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	Lumen's existing commercial and Government security services themselves demand stringent CA controls. Accordingly, CA controls for EIS BSS will be built upon our security assessment and authorization policies and approval procedures already in place.
CA-2	Security Assessments	CA-2 (1)	
CA-3	System Interconnections	CA-3 (5)	
CA-5	Plan of Action and Milestones	CA-5	
CA-6	Security Authorization	CA-6	
CA-7	Continuous Monitoring	CA-7 (1)	
CA-9	Internal System Connections	CA-9	

Figure 8.2.2.2-5. Security Configuration Management (CM) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CM-1	Configuration Management Policy and Procedures	CM-1	EIS Services' CM controls will be built upon Lumen's existing CM policies and approval procedures.
CM-2	Baseline Configuration	CM-2 (1) (3) (7)	
CM-3	Configuration Change Control	CM-3 (2)	
CM-4	Security Impact Analysis	CM-4	
CM-5	Access Restrictions for Change	CM-5	
CM-6	Configuration Settings	CM-6	
CM-7	Least Functionality	CM-7 (1) (2) (4)	
CM-8	Information System Component Inventory	CM-8 (1) (3) (5)	
CM-9	Configuration Management Plan	CM-9	
CM-10	Software Usage Restrictions	CM-10	
CM-11	User-Installed Software	CM-11	

Figure 8.2.2.2-6. Contingency Planning (CP) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CP-1	Contingency Planning Policy and Procedures	CP-1	Operating critical national infrastructure, Lumen has robust CP controls in place. EIS BSS CP controls will be built upon these existing CP policies and approval procedures.
CP-2	Contingency Plan	CP-2 (1) (3) (8)	
CP-3	Contingency Training	CP-3	
CP-4	Contingency Plan Testing	CP-4 (1)	
CP-6	Alternate Storage Site	CP-6 (1) (3)	
CP-7	Alternate Processing Site	CP-7 (1) (2) (3)	
CP-8	Telecommunications Services	CP-8 (1) (2)	
CP-9	Information System Backup	CP-9 (1)	
CP-10	Information System Recovery and Reconstitution	CP-10 (2)	

Figure 8.2.2.2-7. Identification and Authorization (IA) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
IA-1	Identification and Authentication Policy and Procedures	IA-1	EIS BSS IA controls will be built upon Lumen's existing IA policies and approval procedures.
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (2) (3) (8) (11) (12)	
IA-3	Device Identification and Authentication	IA-3	
IA-4	Identifier Management	IA-4	
IA-5	Authenticator Management	IA-5 (1) (2) (3) (11)	
IA-6	Authenticator Feedback	IA-6	
IA-7	Cryptographic Module Authentication	IA-7	
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	

Figure 8.2.2.2-8. Incident Response (IR) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
IR-1	Incident Response Policy and Procedures	IR-1	As for other control families, Lumen's existing commercial and Government security services themselves demand stringent IR controls. EIS BSS IR controls will be built upon Lumen's existing IR policies and approval procedures.
IR-2	Incident Response Training	IR-2	
IR-3	Incident Response Testing	IR-3 (2)	
IR-4	Incident Handling	IR-4 (1)	
IR-5	Incident Monitoring	IR-5 (1)	
IR-6	Incident Reporting	IR-6 (1)	
IR-7	Incident Response Assistance	IR-7 (1)	
IR-8	Incident Response Plan	IR-8	

Figure 8.2.2.2-9. Maintenance (MA) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
MA-1	System Maintenance Policy and Procedures	MA-1	EIS BSS MA controls will be built upon Lumen's existing MA policies and approval procedures.
MA-2	Controlled Maintenance	MA-2	
MA-3	Maintenance Tools	MA-3 (1) (2)	
MA-4	Nonlocal Maintenance	MA-4 (2)	
MA-5	Maintenance Personnel	MA-5	
MA-6	Timely Maintenance	MA-6	

Figure 8.2.2.2-10. Media Protection (MP) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
MP-1	Media Protection Policy and Procedures	MP-1	EIS BSS MP controls will be built upon Lumen's existing MA policies and approval procedures.
MP-2	Media Access	MP-2	
MP-3	Media Marking	MP-3	
MP-4	Media Storage	MP-4	
MP-5	Media Transport	MP-5 (4)	
MP-6	Media Sanitization	MP-6	
MP-7	Media Use	MP-7 (1)	

Figure 8.2.2.2-11. Physical and Environmental Protection (PE) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	EIS BSS PE controls will be built upon Lumen's existing PE policies and approval procedures in place and will take advantage of the controls and capabilities of Lumen data centers.
PE-2	Physical Access Authorizations	PE-2	
PE-3	Physical Access Control	PE-3	
PE-4	Access Control for Transmission Medium	PE-4	
PE-5	Access Control for Output Devices	PE-5	
PE-6	Monitoring Physical Access	PE-6 (1)	
PE-8	Visitor Access Records	PE-8	
PE-9	Power Equipment and Cabling	PE-9	
PE-10	Emergency Shutoff	PE-10	
PE-11	Emergency Power	PE-11	
PE-12	Emergency Lighting	PE-12	
PE-13	Fire Protection	PE-13 (3)	
PE-14	Temperature and Humidity Controls	PE-14	
PE-15	Water Damage Protection	PE-15	
PE-16	Delivery and Removal	PE-16	
PE-17	Alternate Work Site	PE-17	

Figure 8.2.2.2-12. Planning (PL) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PL-1	Security Planning Policy and Procedures	PL-1	All EIS Services and the BSS environment benefit from the Lumen product development process that incorporates feedback from all relevant parties, obtains executive support and funding approval, and leverages our
PL-2	System Security Plan	PL-2 (3)	
PL-4	Rules of Behavior	PL-4 (1)	
PL-8	Information Security Architecture	PL-8	

			internal Architectural Best Practices. The process also includes operations and support organizations, including the security organization, which will establish the planning controls.

Figure 8.2.2.2-13. Personnel Security (PS) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PS-1	Personnel Security Policy and Procedures	PS-1	The existing WITS 3 and Networx Enterprise PS controls will serve as the baseline for the EIS Services PS controls.
PS-2	Position Risk Designation	PS-2	
PS-3	Personnel Screening	PS-3	
PS-4	Personnel Termination	PS-4	
PS-5	Personnel Transfer	PS-5	
PS-6	Access Agreements	PS-6	
PS-7	Third-Party Personnel Security	PS-7	
PS-8	Personnel Sanctions	PS-8	

Figure 8.2.2.2-14. Risk Assessment (RA) Controls Family.

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
RA-1	Risk Assessment Policy and Procedures	RA-1	EIS BSS will build upon Lumen's Risk Assessment policies and approval procedures already in place.
RA-2	Security Categorization	RA-2	
RA-3	Risk Assessment	RA-3	
RA-5	Vulnerability Scanning	RA-5 (1) (2) (5)	

Figure 8.2.2.2-15. System and Services Acquisition (SA) Controls Family

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SA-1	System and Services Acquisition Policy and Procedures	SA-1	EIS BSS will build upon the systems acquisition policies and budget approval procedures in place for Lumen and a SCRM plan to meet these controls.
SA-2	Allocation of Resources	SA-2	
SA-3	System Development Life Cycle	SA-3	EIS BSS already in place in support of WITS 3 and Networx Enterprise contracts and those to be developed

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
			have been or will be designed per the Lumen Product Development Process in which all appropriate parties are included from the inception phase through operation and decommissioning. The security operations and compliance teams are involved, as well as the legal department, procurement and the executive team.
SA-4	Acquisition Process	SA-4 (1) (2) (9) (10)	
SA-5	Information System Documentation	SA-5	
SA-8	Security Engineering Principles	SA-8	Lumen employs Security Engineering principals consistent with a large telecommunications provider and as outlined in NIST SP 800-27. Such principals emphasize support for industry standards, global scale, and deny by default.
SA-9	External Information System Services	SA-9 (2)	
SA-10	Developer Configuration Management	SA-10	
SA-11	Developer Security Testing and Evaluation	SA-11	

Figure 8.2.2.2-16. System and Communications Protection (SC) Controls Family.

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SC-1	System and Communications Protection Policy and Procedures	SC-1	EIS BSS SC controls will build upon Lumen's existing SC policies and approval procedures for our security services for commercial and Government customers. If and where required, FIPS certified cryptography will be used.
SC-2	Application Partitioning	SC-2	
SC-4	Information in Shared Resources	SC-4	
SC-5	Denial of Service Protection	SC-5	
SC-7	Boundary Protection	SC-7 (3) (4) (5) (7)	
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)	
SC-10	Network Disconnect	SC-10	
SC-12	Cryptographic Key Establishment and Management	SC-12	
SC-13	Cryptographic Protection	SC-13	
SC-15	Collaborative Computing Devices	SC-15	
SC-17	Public Key Infrastructure Certificates	SC-17	

SC-18	Mobile Code	SC-18	
SC-19	Voice Over Internet Protocol	SC-19	
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20	
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	
SC-23	Session Authenticity	SC-23	
SC-28	Protection of Information at Rest	SC-28	
SC-39	Process Isolation	SC-39	

Figure 8.2.2.2-17. System and Information Integrity (SI) Controls Family.

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SI-1	System and Information Integrity Policy and Procedures	SI-1	EIS BSS will Leverage the System Integrity policies and approval procedures in place for Lumen. If and where required, FIPS certified cryptography will be used.
SI-2	Flaw Remediation	SI-2 (2)	
SI-3	Malicious Code Protection	SI-3 (1) (2)	
SI-4	Information System Monitoring	SI-4 (2) (4) (5)	
SI-5	Security Alerts, Advisories, and Directives	SI-5	
SI-7	Software, Firmware, and Information Integrity	SI-7 (1) (7)	
SI-8	Spam Protection	SI-8 (1) (2)	
SI-10	Information Input Validation	SI-10	
SI-11	Error Handling	SI-11	
SI-12	Information Handling and Retention	SI-12	
SI-16	Memory Protection	SI-16	

NIST SP 800-53 Rev. 4 also defines controls that are independent of any system impact level such as those pertaining to Program Management (**Figure 8.2.2.2-18**). Lumen is very well positioned with a strong and security-aware program management organization.

Figure 8.2.2.2-18. Program Management (PM) Controls Family

CNTL NO.	CONTROL NAME	COMMENTS
PM-1	Information Security Program Plan	Lumen EIS BSS will have a team of Lumen employees dedicated to the Program Management support and success
PM-2	Senior Information Security Officer	

PM-3	Information Security Resources	of the contract. Teams are tasked with developing the Information Security Program, as well as maintaining the POA&M and managing the interactions with the rest of the Lumen systems and processes.
PM-4	Plan of Action and Milestones Process	
PM-5	Information System Inventory	
PM-6	Information Security Measures of Performance	
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	
PM-10	Security Authorization Process	
PM-11	Mission/Business Process Definition	
PM-12	Insider Threat Program	
PM-13	Information Security Workforce	
PM-14	Testing, Training, and Monitoring	
PM-15	Contacts with Security Groups and Associations	
PM-16	Threat Awareness Program	

Privacy Controls (**Figure 8.2.2.2-19**) are also defined as independent of any system impact level. Again, Lumen is very well positioned with well established privacy controls that are required across much of our business.

Figure 8.2.2.2-19. Privacy Controls

ID	PRIVACY CONTROLS	ID	PRIVACY CONTROLS
AP	Authority and Purpose	DM-2	Data Retention and Disposal
AP-1	Authority to Collect	DM-3	Minimization of PII Used in Testing, Training, and Research
AP-2	Purpose Specification	**IP**	**Individual Participation and Redress**
AR	Accountability, Audit, and Risk Management	IP-1	Consent
AR-1	Governance and Privacy Program	IP-2	Individual Access
AR-2	Privacy Impact and Risk Assessment	IP-3	Redress
AR-3	Privacy Requirements for Contractors and Service Providers	IP-4	Complaint Management
AR-4	Privacy Monitoring and Auditing	**SE**	**Security**
AR-5	Privacy Awareness and Training	SE-1	Inventory of Personally Identifiable Information
AR-6	Privacy Reporting	SE-2	Privacy Incident Response
AR-7	Privacy-Enhanced System Design and Development	**TR**	**Transparency**
AR-8	Accounting of Disclosures	TR-1	Privacy Notice

ID	PRIVACY CONTROLS	ID	PRIVACY CONTROLS
DI	**Data Quality and Integrity**	TR-2	System of Records Notices and Privacy Act Statements
DI-1	Data Quality	TR-3	Dissemination of Privacy Program Information
DI-2	Data Integrity and Data Integrity Board	**UL**	**Use Limitation**
DM	**Data Minimization and Retention**	UL-1	Internal Use
DM-1	Minimization of Personally Identifiable Information	UL-2	Information Sharing with Third Parties

8.2.2.3 Monitoring Strategy, RMF Task 2-3

Lumen utilizes a continuous monitoring strategy to ensure the EIS Boundary is maintained and managed based on the categorization definition. Lumen reports on the security state of the system to appropriate organizational officials via a quarterly POAM as well as an Annual Assessment.

The Lumen security department and system designers are identifying the monitoring activities and targets that must be in place as we finalize our system design and select our suppliers. This design and selection process includes monitoring tools and techniques. As practical, we expect to automate the monitoring process as only automation can provide near real-time monitoring.

As with controls, Lumen can build its monitoring strategy for EIS BSS on that of other Lumen systems including the Lumen Networx Portal.

8.2.2.4 Security Plan Approval, RMF Task 2-4

Although many of its elements are well understood and will be predicated on existing monitoring activities and controls, the BSS Security Plan remains in development and will be completed and delivered to GSA within 30 days from NTP in accordance with EIS RFP Section G.5.6.4.

8.2.3 Step 3: Implement Security Controls

Dedicated personnel responsible for the management of the boundary will be used to implement the security controls and with assistance from Information System Security Officer/ Information Systems Security Manager (ISSO/ISSM), the EIS BSS

SSP will be developed to document relevant policies, process and controls. Attributes include:

- Policy, Process Creation
- Control Implementation – Center for Internet Security/security technical implementation guides (CIS/STIG) Checks, Boundary Validation

By virtue of the high degree of control overlap between EIS BSS and other Lumen systems, security control implementation will be much easier than if we had no baseline from which to work. At this time, we are reviewing security controls that can be classified as common controls and are not likely to be influenced by supplier selection such as PE controls.

In implementing security controls, Lumen adheres to the following set of internal guidelines for each control:

- **Description**: The control's implementation and how it satisfies the security requirement are described.
- **Responsibility**: The people (or person) responsible for implementing and enforcing the control solution are named.
- **Review Policy**: The periodicity (daily, weekly, monthly, etc.) for reviewing the control and its implementation is specified. This information includes the naming of who conducts the review and what initiates it. The review initiation can be according to a schedule and/or an event.
- **Documentation**: Specify how reviews are documented and how we prove that the control is implemented and reviewed. If a published policy is the basis for the control's implementation, then that policy will be included with the documentation.

8.2.4 Step 4: Assess Security Controls

Lumen ISSO/ISSM will execute an assessment of systems in the boundary in compliance with 800-53 and 800-53A assessment procedures to ensure the security

controls were implemented as designed and operating as expected prior to initiating the EIS A&A process. Attributes include:

- Audit and Assessment
- Mitigation and Remediation
- Re-assessment
- Package submission
- Security Assessment Report
- Remediation

The assessment plan has two phases:

- **Phase 1**: Our internal IT Development teams will review the operational controls and implementation of the technical controls, and then perform vulnerability scanning of the system to ensure that it is functioning as designed.
- **Phase 2**: Members of the Lumen Security team not involved with the design and build of Lumen's GSA Customer Portal perform additional vulnerability testing and operational analysis to verify IT Development and Testing Team's findings.

8.2.5 Step 5: Authorize Information System (EIS BSS)

Once our internal assessment activities are completed, Lumen will seek to authorize the system through GSA.

8.2.6 Step 6: Monitor Security Controls

As noted above in Section 8.3.2.3, we expect to automate the monitoring process to a practical level as only automation can provide near real-time monitoring. Lumen will utilize continuous monitoring strategy to ensure that EIS Boundary is maintained and managed based on categorization definition. Will report on the security state of the system to appropriate organizational officials via a quarterly POAM as well as Annual Assessment.

8.3 BSS System Security Plan (SSP) [G.5.6.4]

The BSS SSP for the information system will initially be completed and submitted within 30 days of the NTP to include annual updates. At a minimum, Lumen will create, maintain and update the following security A&A documentation:

Lumen will develop and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. The BSD for the information system shall initially be completed and submitted within 15 days of the NTP to include annual updates.

Lumen will develop and maintain Interconnection Security Agreements (ISA) developed in accordance with NIST SP 800-47. We will provide any ISAs for the information system with the initial security A&A package to include annual updates.

The Lumen Team will develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Using the template provided in RFP Section J.8, Column E of the workbook titled “Contractor Implemented Settings” will document all Lumen-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate. Lumen will provide a Control Tailoring Workbook for the information system with the initial security A&A package to include annual updates.

Lumen will develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Using the template provided in RFP Section J.8, Lumen will provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package to include annual updates.

Lumen will develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk” and GSA Order CIO 2104.1, “GSA IT General Rules of Behavior.”

Lumen will provide an RoB for the information system with the initial security A&A package to include annual updates.

Lumen will develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” We will provide a System Inventory for the information system with the initial security A&A package to include annual updates.

Lumen will provide a Contingency Plan (CP), Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) for the information system with the initial security A&A package to include annual updates.

Lumen will provide an Contingency Plan Test Plan (CPTP) for the information system with the initial security A&A package to include annual updates.

Lumen will provide a Contingency Plan Test Report (CPTR) for the information system with the initial security A&A package to include annual updates.

Lumen will provide a Privacy Impact Assessment (PIA) for the information system with the initial security A&A package to include annual updates.

Lumen will provide a Configuration Management Plan (CMP) for the information system with the initial security A&A package to include annual updates.

Lumen will develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). We will provide a well-defined, documented, and up-to-date specification to which the information system is built. Lumen will provide the System Baseline Configuration for the information system as a part of the CMP and will be submitted with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9).

Lumen will develop and maintain System Configuration Settings (Reference: NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). We will establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode

consistent with operational requirements. Systems will be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practices in hardening systems, as deemed appropriate by the AO. System configuration settings will be included as part of the Configuration Management Plan and will be updated and/or reviewed on an annual basis.

Lumen will provide an Incident Response Plan (IRP) for the information system with the initial security A&A package to include annual updates. We will test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). Lumen will provide an IRTR for the information system with the initial security A&A package to include annual updates.

Lumen will develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of information system will be accomplished. We will provide a Continuous Monitoring Plan for the information system with the initial security A&A package to include annual updates.

All scans associated with the Plan of Action and Milestones (POA&M) will be performed as an authenticated user with elevated privileges. Scans will include all networking components that fall within the security accreditation boundary.

If applicable, a Code Review Report will be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code and on an annual basis.

Lumen will allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”

All critical and high-risk vulnerabilities will be mitigated within 30 days and all moderate risk vulnerabilities will be mitigated within 90 days from the date vulnerabilities

are formally identified. Updates will be provided on a monthly basis on the status of all critical and high vulnerabilities that have not been closed within 30 days.

Lumen will deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation."

8.4 Additional Security Requirements [G.5.6.6]

Lumen will ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1.

The deliverables identified in RFP Section G.5.6.4 will be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor-selected designation per document sensitivity.

Lumen will cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government's agent.

In accordance with the FAR (RFP Section I, 52.239-1) Lumen will be responsible for the following privacy and security safeguards:

Lumen will not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by Lumen under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by Lumen, we will provide the government logical and physical access to Lumen's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

Automated audits will include, but are not limited to, the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans

- Internal and external penetration testing

Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If Lumen chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans. In these cases, scanning tools and their configurations will be approved by the government. The results of Lumen-conducted scans will be provided, in full, to the government.

Lumen will perform personnel security/suitability in accordance with FAR Part 52.204-9.

9.0 NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN [L.30.2.8, G.11.1-3, F.2.1 (83)]

Purpose

This plan identifies the administrative, technical and operational aspects of the NS/EP functional requirements and how Lumen implements them for the services and CBSAs awarded on the EIS contract.

9.1 Introduction and Overview [G.11]

NS/EP Highlights

- Lumen's EIS services, designed with redundancy, support the critical needs of the Government under conditions of stress
- Lumen's Business Continuity Program ensures the Government of a EIS partner that is always ready to support the objectives of NS/EP
- Lumen successfully supports the Government's TSP through existing processes and procedures

In accordance with the Executive Office of the President, Congress, the Department of Homeland Security (including the Office of Emergency Communications), and other entities of the Government, and issued by the National Communications System (NCS), Lumen developed a robust National Security/Emergency Preparedness (NS/EP) plan. As part of our nationwide telecommunications network, the continuation of services is a critical attribute—especially during times of National Emergency.

The definition of National Emergency includes anything that could cause serious harm to a sizeable segment of the United States population, creates widespread property damage, or shuts down or compromises the ability of the U.S. Government to function. During such disasters, the only remaining link could potentially be that of the national telecommunications infrastructure. Therefore, the Government requires that the National Telecommunications Infrastructure to be resilient during such disasters. Lumen's EIS Contractor Program Management Organization (CPMO) will notify the Government immediately when events arise that may have major consequences to its network. While the GSA CO will set priorities, Lumen will be solely responsible for network operations. **Figure 9.1-1** shows our features and benefits of our NS/EP Plan.

Figure 9.1-1. Features and Benefits of Lumen's NS/EP Plan

FEATURES	BENEFITS
• Lumen has a fully functioning Business Continuity Disaster Recovery (BCDR) system in place supporting existing GSA programs. • The BCDR contains incident detection and protection, response, recovery and improvement.	• Ensure that a documented and tested disaster recovery plan is in use for all users of the GSA EIS program. • Providing peace of mind for all users of the GSA EIS program.
• Fully redundant network across many services and locations serving the Federal Government.	• Keep GSA and its customer's critical communications networks on line to accomplish their mission
• Lumen systems are efficient and in many cases recovery takes place without end user intervention • Proactive monitoring on critical services provides for fast recovery.	• GSA and the Agencies under the EIS program can count on Lumen's robust recovery processes and systems to manage outages and emergencies without customer intervention.
• Lumen's EIS Contractors Program Management Office (CPMO) fully participates in the BCDR planning. • Lumen CPMO provides statistics including on time service delivery and maintenance as well as after action reports to GSA during and following any events that trigger a national emergency.	• GSA and EIS customers will receive scheduled updates and feedback on performance through the BCDR communications plan. • Escalations are handled efficiently. • Lumen CPMO is the single point of contact for the flow of information minimizing confusion during an emergency.

Lumen supports GSA's objective of providing assurance for Government users that services and other service elements acquired from Lumen through EIS will be in compliance with national policy throughout the life of the contract. Lumen ensures that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. Specific national policy requirements include, but are not limited to PL93-288 (Disaster Preparedness Assistance dated May 22 1974), PPD-1 (Organization of the National Security Council System dated February 13, 2009), PPD-21 (Critical Infrastructure Security and Resilience, dated February 12, 1023), NSDD-97, NSDD-145, and other applicable laws, regulations, and directives. Executive Orders (EO) 12472 and 13618 will also be considered in the design and operations of services to be provided under this contract.

Lumen addresses NS/EP requirements within our Business Continuity Program (BCP). The mission of Lumen's BCP is to:

- Identify the threats/hazards and their potential impacts and provide a framework for building enterprise resilience
- Safeguard employees, key stakeholders, and long-term market share in the event of an unplanned interruption to the business
- Maintain uninterrupted service whenever possible and, when necessary, coordinate recovery from unavoidable disruptions quickly and efficiently
- Respond to emergency situations in a safe, effective and timely manner

The key principles of Lumen's BCP include:

- **Incident Prevention** – Protecting services from threats (environment, hardware/software, operational errors, malicious attacks and natural disasters)
- **Incident Detection** – Detecting incidents at the earliest opportunity to minimize impact
- **Response** – Responding to incidents in the most appropriate manner providing for an efficient recovery and minimizing downtime
- **Recovery** – Implementing appropriate recovery strategies and solutions that ensure timely and prioritized resumption of operations
- **Improvement** – Incorporating lessons learned from incidents, exercises and tests to enhance our level of preparedness

Figure 9.1-2 represents the planning and response framework utilized in the program. It represents the proactive planning that is put into place and tested so when actual events occur, Lumen's Incident Management structure coordinates the tactical recovery.

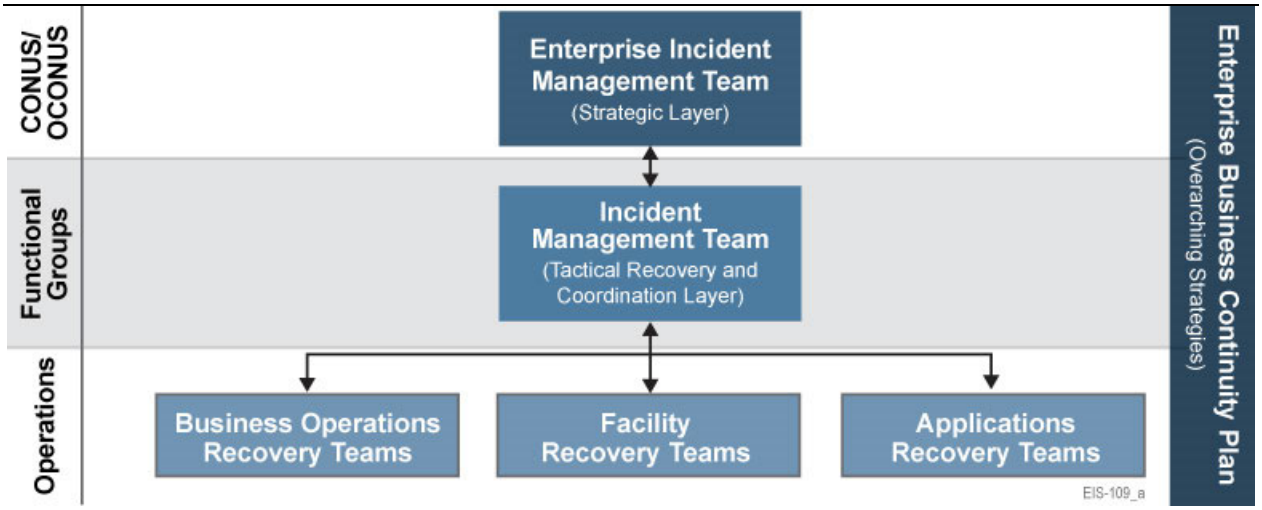


Figure 9.1-2. BCP planning and response framework. *Ensuring a systematic response to incidents.*

9.1.1 Basic Functional Requirements [G.11.1]

In this section we discuss how we meet the basic 14 functional requirements in EIS RFP Section G.11.1. The applicable functional requirements of each service are listed below with comments following each requirement. Since these services are provided using a single network system, the requirements are usually met in the same way for all services provided.

9.1.1.1 Enhanced Priority Treatment [G.11.1 (1)]

Lumen voice and data services supporting NS/EP missions will be provided preferential treatment over other traffic. Lumen follows given intervals for Routine, Class B expedited orders and Telecommunications Service Priority (TSP) orders. We also have built our Trouble and Complaint Handling processes to handle TSP services, based on the assigned restoration priority.

Within the Lumen services, various levels of prioritization and protection are available, depending on the service. For example, Internet Protocol Service (IPS) can be provisioned in either unprotected or protected mode. For all circuits of a critical nature, protected installations are a best practice. In addition, TSP is also available for high-profile access loops.

Critical VoIP links can be provisioned with redundant diverse access links to protect against unforeseen disasters. In fact, disasters such as hurricanes have taken thousands of time division multiplex (TDM) public switched telephone network (PSTN) users out of service, while Voice over Internet Protocol (VoIP) lines that routed traffic via Internet Protocol (IP) backbones remained intact.

9.1.1.2 Secure Networks [G.11.1 (2)]

Lumen provides agency networks with protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.

The Lumen IPS offering is inherently protected against unauthorized access. It is a MultiProtocol Label Switching (MPLS) service, and therefore uses secure label-switched paths (LSP) that are all logically separated into tunneled, logical pipes. Access to such pipes is not possible, except at the sender and receiver end points. The user authentication database, RADIUS, is stored in secured facilities, and the database is backed up and mirrored across locations.

The Lumen Internet Protocol Voice Service (IPVS) offering is supported by a full suite of managed security service options that are inherent in our Virtual Private Network Service (VPNS) service. For example, managed firewalls enable Agencies to separate VPNS services from one another while also providing managed and secure interoperability of designated and agreed-upon applications. Lumen uses intrusion detection and response service to monitor an agency's VPNS service for intrusion events and remediate as appropriate where by each customer's routes are protected; separate VPNS Traffic Queuing, which assigns IPVS traffic a higher priority than Internet traffic; and IPSec Encryption, which effectively hides traffic on our backbone.

9.1.1.3 Non-Traceability [G.11.1 (3)]

Lumen ensures that selected users are able to use NS/EP services without risk of their usage being traced (i.e., without risk of user or location being identified). NS/EP Number Translation (NT) Non-Traceability Voice Service provides critical users the

ability to eliminate the capture of call detail records and caller identification, making calls nontraceable.

For SIP based services, outbound caller ID can be blocked. Calling line ID blocking enables a user to block delivery of their identity to the called party. The user controls the service via a Web interface, which provides the ability to activate and deactivate the service. If activated, all calls made by the user have the user's identity blocked. If this service is activated, users can still choose to allow the delivery of their calling line ID on a specific call by entering the respective feature access code (*65 is the default) for calling line ID delivery per call. Once the call is over, calling line ID blocking is restored.

For TDM (ISDN PRI) based services, there is a feature called "all call privacy." This is all or nothing - any outbound call over the ISDN PRI will have caller ID blocking.

Lastly, most PBXs or IP PBXs have the ability to block caller ID at the telephone number level regardless if the service is SIP or TDM based.

9.1.1.4 Restorability [G.11.1 (4)]

Should a service disruption occur, the Lumen Team voice and data services can be re-provisioned, repaired, or restored to required service levels on a priority basis.

The Lumen geographic network diversity is the core design characteristic driving Lumen's high level of network reliability and restorability. Each city along the network is served by two, or in some cases three, distinct paths, which ensures that a fiber cut along any one route will not isolate a city from the network. The Lumen geographic route diversity has been carefully engineered in the long-haul network, metro network, and gateway entry vaults to ensure maximum separation with minimal spurs or crossings. Most networks are not engineered to these standards.

Additionally Lumen support of the TSP program enables services to be re-provisioned, repaired or restored on a priority basis ahead of other customer services.

9.1.1.5 International Connectivity [G.11.1 (5)]

Lumen is experienced in establishing and managing voice and data services that provide access to and egress from international carriers. Lumen has established an extensive capability in the arena of international interconnectivity. Our business and service model as a "carrier's carrier" has resulted in our robust interconnection agreements that span the globe. We provide services to and have interconnectivity with most major international carriers. Our European facilities based network is fully interconnected with major carriers and has effectively provided business continuity for many carriers and customers in outage. The Lumen customer base representing international connectivity includes:

- Our network is in 60 countries and growing, with worldwide connectivity through interconnection agreements with more numerous foreign carriers
- The world's 10 largest telephone companies
- The 10 largest carriers in Europe and AsiaPAC
- International wireless companies with more than 260 million subscribers

9.1.1.6 Interoperability [G.11.1 (6)]

Lumen and its team members have nearly two decades of experience in ensuring that their voice and data services solutions can interconnect and interoperate with other Government or private facilities, systems, and networks, often when the exact systems were not identified after contract award.

The Lumen IPVS service is based on our Enhanced Local Service (ELS) platform, which uses the same IP backbone to transport voice calls as is used to transport IP packets for our IPS. Since the two use the same underlying transport mechanism—IP packets—they are fully interoperable with one another. Government Agencies can choose to purchase an IP access circuit, and divide the bandwidth up between both voice and data.

9.1.1.7 Mobility [G.11.1 (7)]

The Lumen Team solution includes the ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications. The Lumen network architecture enabling the integration of voice and data infrastructures combined with our mobility partner Managed Mobility supports the dynamic mobility requirements based on the NS/EP user needs.

9.1.1.8 Coverage [G.11.1 (8)]

Based on our experience, we ensure that voice and data services are readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located. **Figure 9.1.1.8-1** shows the major nodes and links of the Lumen backbone.

Our network architecture supports global service coverage that significantly exceeds the minimum CBSA requirements specified in SOW C.1.3. For many of the CBSA-dependent services we cover all 929 CBSAs and we far exceed the coverage minimum for all such services – including an extensive native colocation offering, through which we provide service in Lumen data centers in 63 CBSAs.

The Lumen network based upon our EIS network architecture, not only covers the entire US mainland, but extends to 60 other countries around the globe. Our position as a wholesale carrier and our interconnections with local and regional carriers significantly expands our reach.

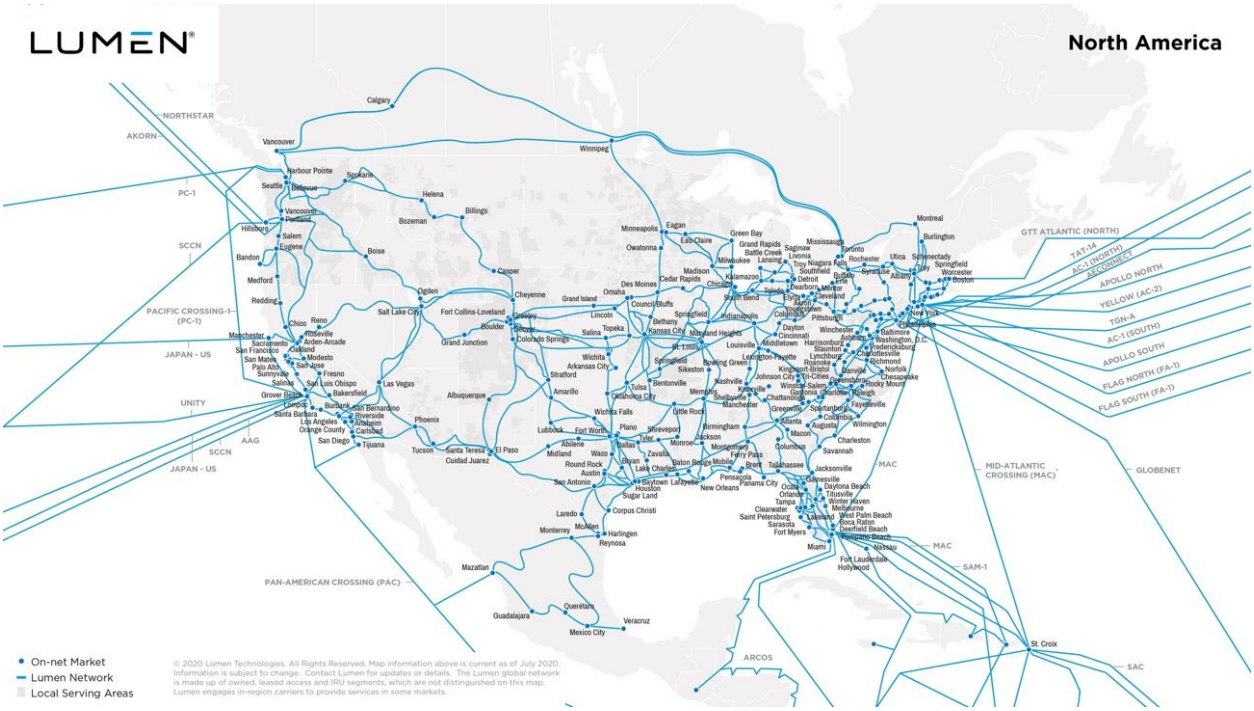


Figure 9.1.1.8-1. Lumen Backbone Major Connectivity Nodes. *The network design supports our diversity and network performance objectives.*

The Lumen reach regarding each of the applicable products extends across the major metropolitan areas of the US, resulting in nationwide coverage. The Lumen network serves 113 on-net markets in the US. In addition, the network delivers wholesale dial-up access coverage to more than 93% of the US population. The network offers voice services in more than 5,700 rate centers nationwide. Our network coverage includes

- We have over 200,000 route miles of fiber; more than 10M fiber miles
- 350 multi-tenant data centers are on-net
- Our network has more than 4,000 network peering points
- On October 31, 2014, Lumen substantially expanded our metro-network reach by acquiring tw telecom, which served approximately 80 U.S. markets

9.1.1.9 Survivability/Endurability [G.11.1 (9)]

Lumen provides voice and data services that are sufficiently robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war. Survivability is a built-in concept with Lumen's BCDR program. It is included with all services provided under the EIS program. The ongoing Risk Management Program calls for preventive measures that reduce the likelihood of disaster—and minimize the impact if one does occur.

9.1.1.9.1 Lumen Network

The Lumen network is fully route-diverse and is designed with complete "ring" protection. This design helps ensure that our protected services are fully path-redundant and are not susceptible to outages. The core design characteristic driving Lumen's high-level of network reliability is geographic network diversity. Each city along the network is served by two, or in some cases three, diverse paths, thus ensuring that a fiber cut along any one route will not isolate a city from the network, ensuring continuity of service.

9.1.1.9.2 Network Operating Centers

Redundant Network Operating Centers (NOC) geographically disbursed enable Lumen to identify and isolate causes of potential network disruptions, and quickly coordinate resolution of system outages.

The GovNOCs, located in Broomfield, CO and Atlanta, GA, are staffed with network operation technicians and specialists using an out-of-band network management system to control routing, mitigate outages and restore service. The Lumen Government Security Operations Center (GovSOC) in Phoenix, AZ monitors network security. These elements all combine to reduce the risk of outage to the Government.

9.1.1.9.3 Network Facilities

All critical facilities have plans for recovering their critical infrastructure from loss of access, power, HVAC or employees, etc. We also conduct evacuation drills to protect the life safety of our employees, customers and vendors.

9.1.1.9.4 Data Centers

Alternate Processing Site: Lumen owns and self-manages a geographically dispersed alternate data center, which is utilized when the primary processing capabilities are not available. The alternate data center is a hot site that is comparable in size, power capacity, and HVAC capacity to the primary data center. The alternate data center is equipped with the infrastructure, environment and connectivity to support recovery of its critical systems and applications for essential business functions within their recovery time objectives.

Alternate Storage Site: Numerous data replication strategies are employed by Lumen to manage data storage in a safe and secure manner. Data from our primary data center may be replicated through various technologies to repositories located in our self-managed, geographically dispersed backup data centers. This capability facilitates meeting our recovery time objectives, and mitigates risk of physical access and retrieval of backup information.

Information System Backup: Lumen has implemented a hot standby solution in its alternate processing and storage site. Periodic testing is conducted on media reliability and information integrity.

Information System Recovery: System recovery is sequenced based on criticality of the functions the information systems support and recovery time objectives and recovery point objectives defined by the business. Each information system's failover capability uses recovery solutions designed to meet recovery objectives.

9.1.1.9.5 Supply Chain/Critical Vendors

Lumen critical vendors and suppliers are asked to demonstrate their business resiliency capabilities. This provides Lumen the ability to manage any risk to their supply chain. Lumen incorporates its partners in its BCDR exercise program.

9.1.1.9.6 Pandemic Preparedness

Lumen recognizes its responsibility to our employees, customers and shareholders to minimize the potential for business disruption and recover operations as rapidly as possible should a disruption occur as a result of a pandemic outbreak. Through effective, ongoing preparation and planning, Lumen employees are provided with public and private resources to enhance awareness and recommend precautions.

Lumen maintains both Global and Business Unit Pandemic Influenza Plans, which are integrated into its Business Continuity Program. Pandemic preparedness focuses on:

- Ensuring mission critical functions remain operational
- Personnel remote access and staff reduction contingency strategies
- Providing an appropriate level of awareness for our employees and customers
- Anticipating and responding to our customer's needs and possible disruptions to our supply chain

9.1.1.9.7 Communications

Backup Communications: Lumen has implemented redundant communications capabilities utilizing alternate carriers. Primary and backup conference bridges are supplied by separate vendors using diverse networks and routes. An automated paging system utilized for notifying and communicating during an event, is also geographically redundant.

Remote Network Access: Lumen's network security architecture allows near-immediate and sustained remote access into our internal network to access critical applications and data through any ISP, regardless of provider.

9.1.1.10 Voice Band Service [G.11.1 (10)]

Lumen provides voice band service in support of presidential communications. Lumen provides an Unbundled Network Element known as Line Sharing to support voice band service. Line Sharing provides the means for a Local Service Provider (LSP) to order service configuration that will allow them to place a digital data service on a subscriber loop currently providing analog voice services to an end user. Line sharing consists of a digital data based service provisioned by a Local Service Provider (LSP) and the voice band service provisioned by Lumen.

9.1.1.11 Broadband Service [G.11.1 (11)]

Lumen provides a service solution that uses broadband service in support of NS/EP missions; for example, video, imaging, web access, and multimedia. High-speed broadband services are the cornerstone products of the Lumen suite. These include high-speed links (OC-3, OC-48, and OC-192), and advanced protocols such as multicast, to enable distribution of video and multimedia across the links.

Through our VPNS product, users can run sessions that are completely secured at the low “bit level” while transferring high-level information such as whiteboard and videoconferences. Web access is instantly available to all ISP customers who have requested Internet connectivity.

9.1.1.12 Scalable Bandwidth [G.11.1 (12)]

Lumen’s solution provides NS/EP users with the ability to manage the capacity of the communications services to support variable bandwidth requirements. All NS/EP users can augment their available bandwidth quickly and efficiently. Lumen supports user bandwidth management through rapid response to change orders using established procedures and the ability to prioritize response to groups earmarked as critical users. Lumen has a world-class service activation and field services organization. In addition, our Lumen GSA Customer Portal enables Agencies to order new services or change existing services online. This web-based system delivers all internal Lumen system capabilities, such as reporting and bandwidth provisioning,

directly to Government customers. By extending the Lumen support applications, we empower customers to perform self-service functions using intuitive Web-based tools.

9.1.1.13 Affordability [G.11.1 (13)]

The Lumen provided services leverage network capabilities to minimize cost (e.g., use of existing infrastructure and commercial off-the-shelf (COTS) technologies and services). Lumen maintains competitive prices starting at the physical layer of the network. Our multi-conduit fiber system enables deployment and maintenance of the latest generations of fiber plant. Layered on the fiber, our wavelength systems are continually upgraded to provide the most cost-competitive transport in the industry. The Lumen IP network is a converged MPLS backbone, enabling us to run all of our IP products over the same backbone. The converged backbone gives Lumen economies of scale and simplifies operations for our support staff.

9.1.1.14 Reliability/Availability [G.11.1 (14)]

Lumen ensures that our services perform consistently and precisely according to their design requirements and specifications, and provide high user reliability and confidence. Regardless of whether the customer is using IPS, IPVS, or VPNS, the service is engineered for precise, efficient performance. Lumen prides itself on customer satisfaction and continually upgrades and updates all services. Lumen provides reliability and high availability through network engineering that designs these qualities into the network from the start. Our fiber plant into each Lumen facility is completely diverse, with at least two entrance points in each facility. Diverse fiber routing in the backbone is also used to ensure that fiber damage does not isolate a facility. On the IP network, Lumen maintains two backbone routers and at least two edge routers in each POP. The Lumen capacity planning group uses modeling tools to ensure that the network has sufficient bandwidth even in the event of a fiber cut or wavelength outage.

9.1.2 Protection of Classified and Service Information [G.11.2]

Lumen protects classified documents and materials presented by this contract in accordance with Executive Order 12958, National Security Information and applicable supplemental directives. We further ensure that the instructions of the EIS RFP and subsequent Task Orders are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of the EIS contract. Lumen's experienced Facility Security Officer (FSO) will support the EIS contract to ensure compliance with the protection of classified and service information.

Lumen understands that protecting classified information could include, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and, customer profiles. Additionally, Lumen understands the Government might provide access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. Classified and service information is in various forms, including hardcopy and electronic media and that the level of classification is up to and including Top Secret / SCI and identified by the Government.

Lumen follows and abide by the contract classification requirements set forth in the DD Form 254, the National Industrial Security Program Operating Manual (NISPOM); applicable Intelligence Community Directives (ICD's) protecting Special Compartmented Information (SCI). We also follow, as applicable, all Office of Selective Acquisitions Security Manager (OSM) and Program Security Advisor (PSA) instructions and guidance. Lumen also follows applicable Cognizant Security Agency requirements for access and handling of classified information at accredited Government facilities.

Lumen facilitates agency access and inspections of agency accredited SCI facilities, to include security policies and procedures, and all materials generated or processed under contract. Lumen handles all SCI materials in accordance with special security requirements, furnished by the responsible OSM.

Lumen has extensive experience working sensitive and secure programs. We have the facilities, systems, processes, and personnel to assure full implementation of all National Security measures – be they Department policies, Executive Orders, National Security/Homeland Security Directives, and all other documents, public laws, and specifications. Lumen will follow best commercial practices to protect EIS related information. We voluntarily participate in regional security working groups to assure we stay abreast of best practices, and understand emerging threats. We anticipate a close and cooperative working relationship with regard to protecting classified information as we do on existing programs with certain classified and sensitive information.

9.1.3 Department of Homeland Security (DHS) Office of Emergency Communications Priority Telecommunications Services [G.11.3]

Lumen, whose network is an acknowledged component of the nation's telecommunications critical infrastructure has, in close partnership with the Federal Government, put processes in place to fully coordinate both preparation and response to pending or actual disasters in order to minimize the impact to network assets and services. To further build ties with Government emergency management programs, Lumen is an active participant in the National Communications System's National Coordinating Center for Telecommunications (NCC). The company has a representative on the NCC who regularly participates in national-level coordination meetings, regional exercises, and actual disaster response events to build an effective partnership for responding to emergencies. Such familiarity between Lumen and the Federal Government has paid dividends in managing real-world situations that could result in business disruptions. Additionally, Lumen has formed close working relationships with various departments in the Federal Government, to include the Department of Defense and the DHS, to meet their exacting need for reliable network services under all conditions. BCP is an essential component of the Lumen business operating model. The nature of the telecommunications industry, and the products and services Lumen provides are expected by customers to meet remarkably high standards for availability.

The Lumen Board of Directors respects this responsibility and ensures a robust BCP Program is in place to maintain uninterrupted network service whenever possible and, when necessary, to recover from unavoidable service disruptions quickly and efficiently

9.1.3.1 Government Emergency Telecommunications Service [G.11.3.1]

The Lumen network supports the GETS program by connecting customers to the GETS network in the event of congested voice networks due to emergencies. Lumen also utilizes the GETS program in support of their business continuity disaster recovery plan (BCDR). GETS has the following capabilities:

- GETS is available nationwide and can be accessed from international locations
- GETS can be accessed through the Defense Switched Network, FTS2001/Networx, the Diplomatic Telecommunications Service, and the Federal Emergency Management Agency Switched Network
- GETS calls may be placed from cellular and satellite phones
- GETS access is restricted to individuals with NS/EP responsibilities. Traditionally, users must meet those responsibilities outlined in Executive Order 13618, Assignment of National Security and Emergency Preparedness Communications Functions

9.1.3.2 Wireless Priority Service (WPS) [G.11.3.2]

The Lumen Team fully complies and interoperates with the WPS service as identified in White House-directed emergency phone service managed by the DHS OEC. WPS complies with the Federal Communications Commission (FCC) Second Report and Order, FCC 00-242, Establishment of Rules and Requirements for Priority Access Service. Through our wireless partner Managed Mobility WPS is available wherever T-Mobile provides digital voice service on its Global System for Mobile Communications/Universal Mobile Telecommunications System (GSM/UMTS) network. Users may be able to use WPS while roaming on other GSM/UMTS WPS-enabled networks. WPS is not available when roaming on GSM/UMTS networks that are not WPS-enabled or in service areas not covered by roaming agreements between carriers.

T-Mobile USA through its WPS integration contractor DynCorp, is a WPS contract holder. Nationwide WPS is operational in 15 metropolitan areas in the Eastern U.S., with additional markets to follow. T-Mobile has provided WPS in the greater Washington, D.C. and New York City metropolitan areas since May 2002. WPS enables designated national security and emergency preparedness personnel greatly improved capability to complete wireless calls during times of emergency.

When trying to make a call in times of emergency, WPS users have the ability to queue at the top for the next available capacity from their closest base station ito place their call, greatly enhancing their ability to complete wireless calls during these critical times and assist the situation. WPS is available only to designated leadership at all government levels, national security, emergency responders, and private sector critical infrastructure personnel, as approved by NCS and FCC Rules and Requirements.

In addition to the greater New York City and Washington, D.C. areas, the initial Nationwide WPS capability is now available in metropolitan areas surrounding Atlanta; Birmingham, AL; Boston; Jacksonville, FL; Louisville, KY; Memphis, TN; Miami; Mobile, AL; Nashville, TN; New Orleans; Norfolk, VA; Philadelphia, and Richmond, VA. Additional markets will be added nationwide over the next few months, as will further enhancements to the capability.

9.1.3.3 Telecommunication Service Priority (TSP) [G.11.3.3]

The TSP program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service. Lumen fully complies with the TSP requirements and is well versed in supporting services under the program.

Telecommunications Service Priority

Required criteria for eligible services:

- Serves our national security leadership;
- Supports the national security posture and U.S. population attack warning systems;
- Supports public health, safety, and maintenance of law and order activities;
- Maintains the public welfare and the national economic system; or
- Is critical to the protection of life and property or to NS/EP activities during an emergency.

Lumen has been an ongoing active member of the Telecommunications Service Priority Oversight Committee (TSPOC) for the past several years, including the January 2016 – December 2017 term. The TSPOC has been established to provide advice and assistance to the Manager, Office of Emergency Communications, as the administrator of the TSP Program. As a member of the Committee, the TSPOC helps to ensure that TSP Program operational policies and procedures remain responsive to priority service requirements and that the system remains current with the telecommunications industry technical capabilities. The TSPOC also provides a forum for you and your fellow Committee members to identify, discuss, and recommend solutions to TSP Program issues.

TSP Provisioning

Lumen supports both TSP provisioning activities:

- **Emergency Provisioning.** Telecommunications services in the Emergency NS/EP category are new services so important as to be required to be provisioned at the earliest possible time without regard to cost of obtaining them.
- **Essential Provisioning.** Telecommunications services in the Essential NS/EP category are new services that must be installed by a specific dates and cannot be met under normal business procedures.

When TSP is specified in an order, Lumen ensures the priority intervals prescribed by the agency are met. The provisioning guardrails put in place by Lumen are monitored by three groups ensuring that each interval is met. Those groups are Customer Service Manager (CSM), Customer Care Manager (CCM), and Project Manager (PM). By using the automation inherent in Lumen's critical-date-management tool, each group can manage to the requested date. This tool also provides Lumen access into the subcontractors' progress. Using this automation, Lumen manages all contractors with real-time responses, eliminating the wait time to gather vital information in completing each. There are fields present in the Lumen GSA Customer Portal that

clearly identify a service order to be handled using the TSP process, providing provisioning priority level. **Figure 9.1.3.3-2** is the Provisioning Process for TSP services.

TSP Restoration

When TSP is specified at the restoration level The Lumen Trouble Management processes is also built to handle TSP services, based on the assigned restoration priority. Should Lumen's network experience significant degradation or failure, we will provide priority restoration of affected services in accordance with the TSP system five levels of priorities. As with the service ordering process there are fields present in the Lumen GSA Customer Portal that identifies the restoration priority level. Services that have a TSP restoration priority that are alarmed issue an automatic page out to the Technical Customer Service Representative (TCSR). If our Operations Automation (OA) system generates a ticket on a network alarm that has a TSP restoration priority assigned to the service, the trouble ticket is prioritized ahead of other trouble tickets for resolution.

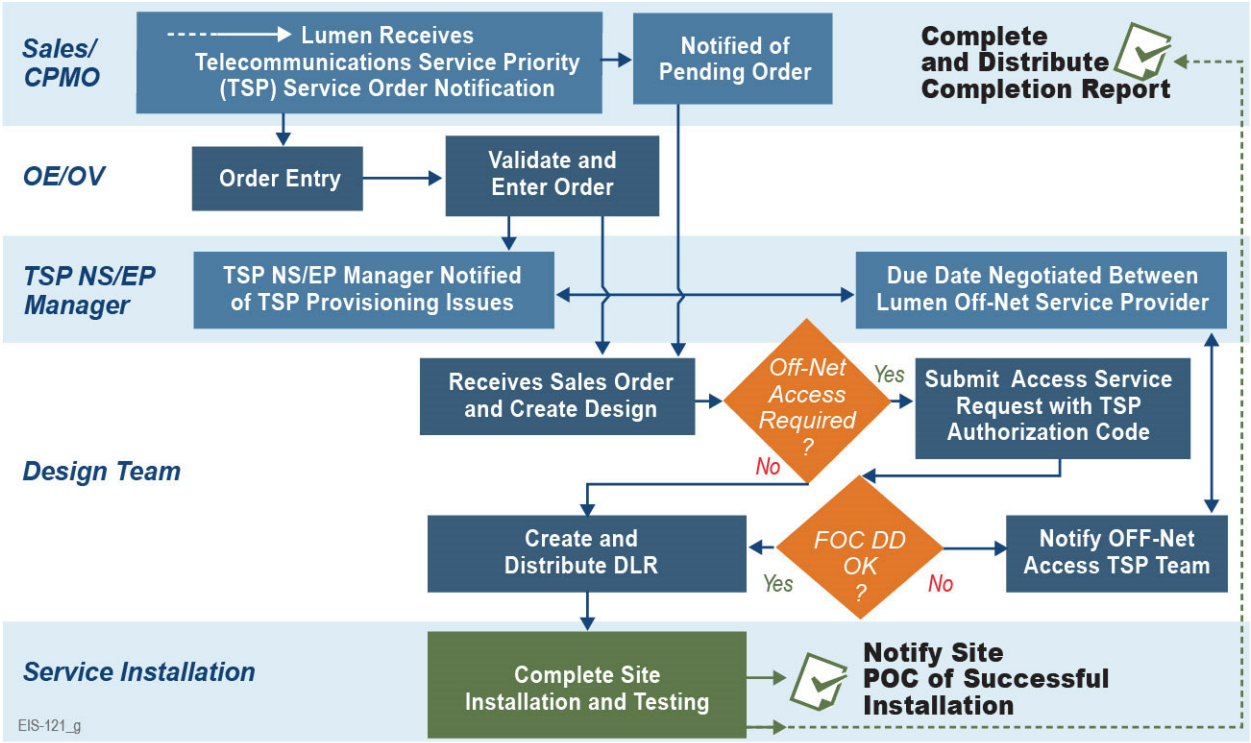


Figure 9.1.3.3-2. NS/EP or Emergency/Essential Provisioning Process.

9.2 Deliverables [F.2.1 (83), G.11.1]

Lumen will provide the following deliverables for this plan noted in **Figure 9.2-1**.

Lumen will collaborate closely with the GSA PMO and EIS customer agencies to ensure that we maintain a current list of deliverables for this plan and review content to ensure compliance with any modifications to the Task Order.

Figure 9.2-1. NS/EP Functional Requirements Implementation Deliverables

ID	REQUIREMENT REFERENCE	DELIVERABLE DESCRIPTION REFERENCE	DELIVERABLE NAME	FREQUENCY	DELIVER TO
83	G.11	G.11	NS/EP Functional Requirements Implementation Plan	Initial: With proposal Update: Annually from contract award	GSA COR