Appendix A

WITS 3 Contingency Plan

(Req_ID 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1070)

Level 3 Communications, LLC

Version 2.1

April 19th, 2007

1.0 CONTINGENCY PLAN INTRODUCTION

Level 3 is providing this Contingency Plan for the WITS 3 proposal, as a deliverable that will be updated yearly. It describes in detail the method by which WITS 3 services will be maintained and restored under a number of emergency situations, and addresses damage assessment, service restoration time frames, and triggering mechanisms. Our Contingency Plan specifies Level 3 emergency maintenance actions to be executed by Level 3, and our emergency equipment replacement arrangements with suppliers and alternate service arrangements with other carriers.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Business Continuity Planning (BCP) is an essential component of the Level 3 business operating model. The nature of the telecommunications industry and the products and services Level 3 provides are expected by customers to meet remarkably high standards for availability. The Level 3 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. This plan sets forth the processes and procedures Level 3 will follow should business be disrupted by a predictable or non-predictable event.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Risk Management: Level 3's BCP program is a critical piece in the enterprise's Risk Management program that is structured to identify, assess, mitigate, and manage the potential effects of business disruptions. Level 3's services have been designed to address risk management by focusing on proactive prevention and mitigation solutions to reduce exposure.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Training and Testing: Level 3 engages in an active exercise program to validate the effectiveness and up-to-date status of recovery processes and plans. All activities are scripted, tested, and reviewed so that recovery times are known and verified in advance of an event. The testing activities range from simple table-top discussions to full-scale simulations of events and may be announced in advance or conducted without advance notice to enhance realism. Exercises are closely monitored by evaluators. At their conclusion, a thorough analysis of exercise results is conducted and documented to identify the strengths and weaknesses in plan conception and implementation and to enable modifications if necessary. Note: We believe that the Level 3 BCP program is appropriate for our business. But because all BCP programs, from time to time, require the support and cooperation of third parties such as government agencies, diesel fuel vendors, and equipment vendors, the success of Level 3's BCP program at times will be dependent upon the cooperation of these third parties.

[redacted]

[redacted]

The specific audience of the Business Continuity Program includes:

[redacted]

2.2 BUSINESS CONTINUITY PLANNING ORGANIZATION

Risk Management Council: The various components of the BCP program receive oversight and direction at the highest management level through the corporate RMC, which is comprised of members from the Level 3 executive management team. The RMC addresses, makes decisions, and assigns resources to manage the security, business continuity, and environmental risks facing Level 3.

Emergency Response Teams: The EIMT enhances the ERT by providing a proactive, centralized communications vehicle when a situation poses a potential risk and aids in allowing preparations to be made for a smooth transition to the ERT in case an event is declared. This team provides a quick and early reaction to possible and actual events, consistency of information to stakeholders, and expertise in disciplines responsible for key aspects of incident response and business continuity.

The Level 3 ERT is activated when internal or external events pose an extraordinary risk that could impact the safety of people, the network, or business assets. The ERT is comprised of senior-level leadership representing key business units and is organized into sub-teams, each of which has defined roles and responsibilities.

Each team represents a function that serves in a critical role during life safety events or business disruptions. The Corporate BCP Office is responsible for facilitating the group and documenting and supporting the functional team members. Each function has a designated primary and alternate to implement recovery strategies and/or action plans. The teams include:

[redacted]

More detail on the composition, roles, responsibilities, and processes of these teams is found in the Concept of Operations section.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

396

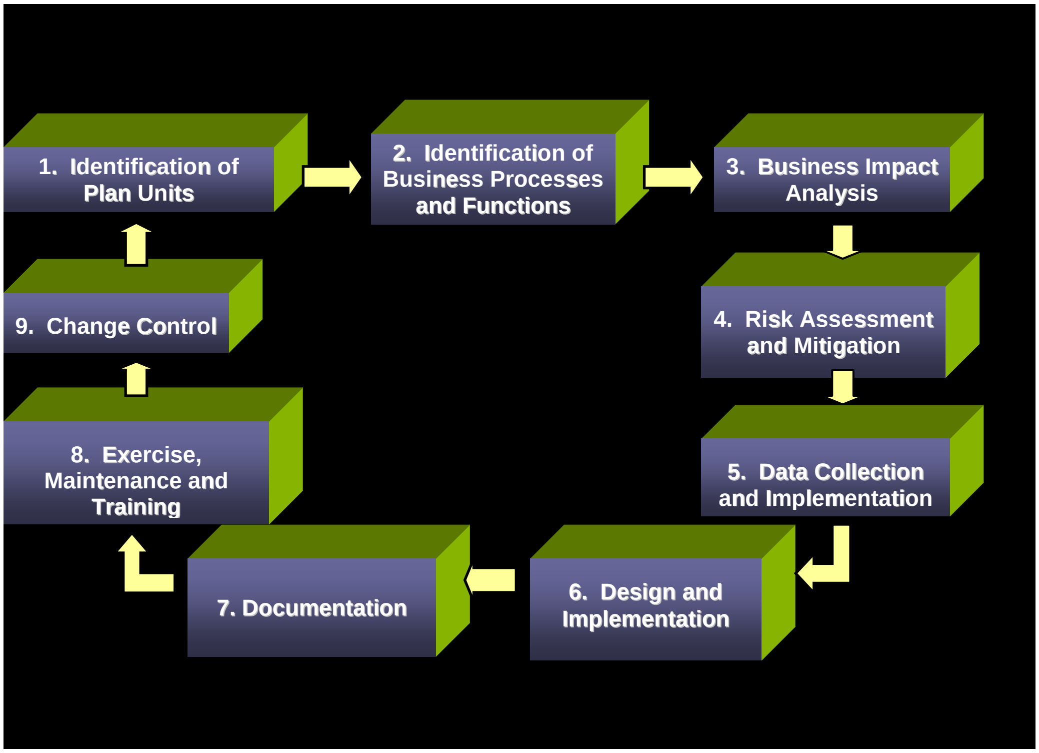
[redacted]

Network Access: Those employees who lose access to their facility can still access the Level 3 Network remotely. Level 3 organizations will coordinate specific requirements through their respective Business Continuity Coordinator (BCC).

[redacted]

[redacted]

[redacted]


1. Identification of Plan Units
2. Identification of Business Processes and Functions
3. Business Impact Analysis
4. Risk Assessment and Mitigation
5. Data Collection and Implementation
6. Design and Implementation
7. Documentation
8. Exercise, Maintenance and Training
9. Change Control

[redacted]

[redacted]

Business Continuity Structure and Process

The Level 3 BCP elements include technology plans, business plans, facilities plans, site-based plans (life and safety), and incident management. When a potential or actual business disruption occurs, the impacted business unit(s) will respond and communicate activity and status to the ERT/EIMT. These teams use an automated communication system capable of activating a team within minutes to rapidly convene the skill sets necessary to resolve potential or actual disruptive events. The designated primary and backup members of the ERT/EIMT, who are principally drawn from the executive level, have in-depth expertise across the enterprise and operate from pre-established plans to manage disruptive events.

The BCP program guides the ERT/EIMT and provides for situation assessment, operational and security response, escalation procedures, and internal and external communications. The ERT/EIMT manages both the emergency response and recovery phases of a disruptive event. Resource requirements for recovery will be communicated by impacted business units to the appropriate ERT/EIMT representative.

Emergency Response: An emergency response is appropriate during and immediately following a business disruption or disaster. The objectives of the process are to ensure the safety and accountability of Employee-Owners (EO's) and those present in affected Level 3 facilities and to assess the nature and scope of the disruption to begin recovery actions. In addition, the ERT/EIMT coordinates the immediate impact of and response to the disaster with appropriate Government emergency management organizations, customers, and other key stakeholders.

Business Continuity: Business continuity begins immediately following the emergency response phase, lasting until normal business functionality has been restored. The process objective is to restore the processes needed for immediate operations and ensure that Level 3 continues to service its customers as needed.

IT Systems Continuity: The continuance of IT systems also begins immediately following the emergency response phase, lasting until IT system functionality and data have been restored. The restoration of the IT systems to established recovery points is the objective of this portion of the process. The team uses a structured, coordinated approach following a recovery sequence that is based on the importance of the IT system to prioritized business processes.

Standards and Assumptions:

This section discusses the standards and assumptions that guide the actions of our business continuity planning processes.

- The first and foremost concern of Level 3 in a business disruption and/or disaster situation is the safety of Employee-Owners and others in our facilities. In addition, we will strive to protect and preserve our assets, network, and customers. As a result of careful planning, the Level 3 NOC, ERT, and EIMT are operational 24 x 7. Level 3 also recognizes that an event could affect any Level 3 facility; thus, plans apply to all facilities.
- Level 3 recognizes that local authorities have command and control over life safety issues in a disaster. A key objective is to ensure that internal and public communications plans are intact.
- Level 3 Business Continuity Plans are written assuming the worst-case scenario (the workplace, all documents, and equipment are inaccessible, and some employees may not be available). If a disaster results in less damage than the worst-case scenario for a facility, Business Continuity Plans will be scaled back accordingly under the direction of the continuity plan owner. However, in any business disruption situation involving a significant impact to the enterprise, the ERT/EIMT will be formed to manage the event.
- The ERT/EIMT will assign resources for recovery based on each business unit's relative priority to the company based on financial, customer, and reputation perspectives. During a disaster, recovery teams will communicate resource requirements to their representative on the ERT/EIMT, who will then coordinate resource assignment.

- Impacted business units have a continuity plan for each facility they manage and documented steps for restoring their business processes and/or IT systems. These plans are available in a variety of ways to each business unit during an event.
- Common infrastructure requirements (i.e., alternate facilities, workspace, IT workstations, telecommunications, and network connectivity) will be provisioned centrally by the appropriate business groups (real estate, facilities, Voice and Softswitch, infrastructure, etc.) based on direction and oversight from the ERT/EIMT. Each impacted business unit is responsible for identifying its resource requirements in the appropriate sections of its continuity plans and for communicating requirements to their representatives on the ERT/EIMT.
- Level 3 stores backup tapes of data from offsite centrally managed servers, which are available within 24 hours. The IT applications have been grouped into two categories for recovery priority: Tier 1 and Tier 2. The most critical IT applications are assigned to Tier 1 with an RTO of 72 hours or less.
- The Level 3 “All Hazard” plan is a document that reflects the changing environment and requirements of Level 3. Therefore, Level 3 continually allocates resources to maintain the BCP program and keep it in a constant state of readiness.

2.3 General Approach

The Level 3 emergency response encompasses identifying the nature of the emerging or existing disaster, evacuating, and accounting for those in the affected facility, if appropriate, notifying the appropriate civil response organizations (fire/police/medical), notifying the appropriate management structure of the situation, and standing by to assist civil authorities and upper management.

Each functional group or business unit is responsible for recovering the business processes that it owns. Emergency response plans at Level 3 are developed and implemented at the facility level. Additionally, recovery will encompass the efforts taking place after the emergency response phase to restore the functionality of business processes in a coordinated, prioritized fashion.

The business teams having IT system administration responsibilities are responsible for recovering the IT systems they administer in concert with the recovery priority of the business processes the IT systems support.

2.3.1 Responsibilities

Each business team that owns facilities, business processes, and/or administers IT systems is responsible for its area of expertise and ownership of their business continuity processes.

- Each team has developed and documented a Business Continuity Plan for the facilities or function it manages. This plan details the continuity of its business processes or systems. In addition, the plan is reviewed at least semi-annually. The business unit executes the plan during exercises and during an actual event.
- Each team also ensures that all people assigned to a continuity team know of the plan's existence, how to access it, and their role within the plan. Copies of the plan are stored outside of LDRPS in either printed or softcopy form and kept off-site so that they are readily available at the time of an event. The team is instructed in the identity of their group's ERT representative (and backups) and how to contact them in an emergency situation. Additionally, the teams know the identity of the people who administer their IT systems/applications and how to contact them in an emergency situation.

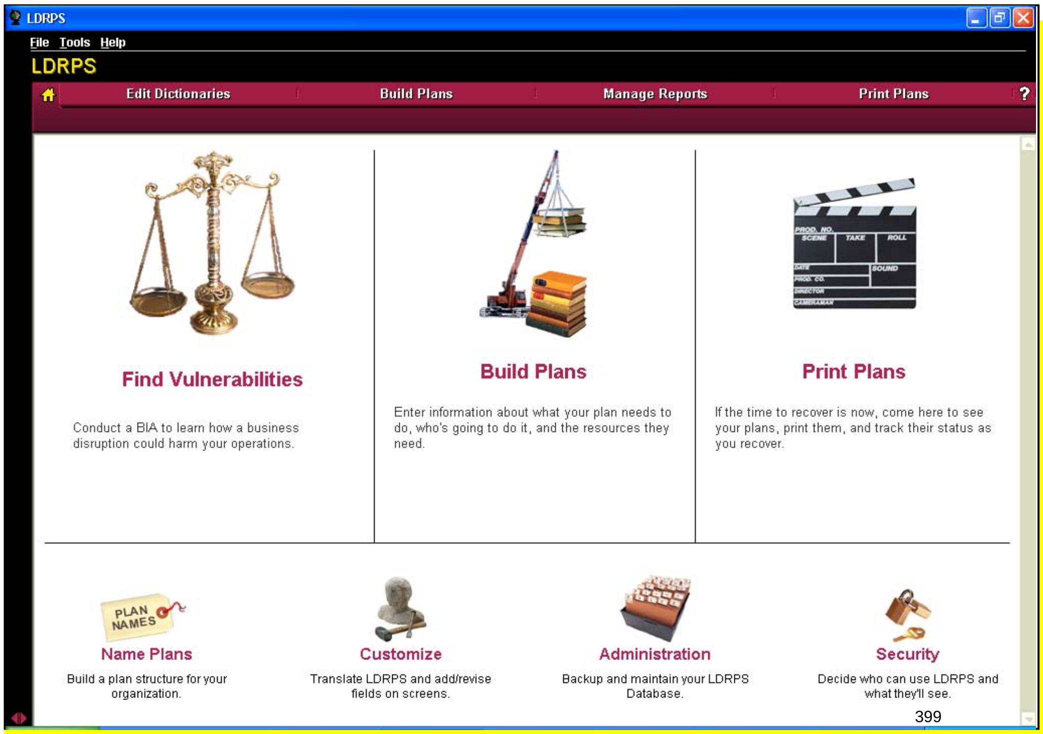
2.3.2 Plan Activation

Activation of emergency response and evacuation plans is the responsibility of the senior employee at a facility at the time of an emergency. Business Continuity Plans are activated under the direction of the Event Manager of the ERT. ***Table A-1*** details the standardized terminology Level 3 uses to develop and manage its business continuity processes.

Standardized Terminology	
Business Continuity Plan	A plan built and maintained by a business unit to guide the recovery and restoration of business processes or IT systems following a business disruption.
Emergency Response Phase	The period of initial response to an event during which time people at the site are removed from harm's way and the damage/impact to the business is assessed.
Recovery Phase	The period following the Emergency Response Phase of a business-disrupting event during which continuity plans are executed. Recovery follows established business continuity plans. The recovery phase continues until a permanent facility is operational, all business processes have been recovered to their pre-disruption state, and business returns to normal operating levels.
Plan Unit	A continuity plan that is comprised of members from a business unit(s) responsible for participating in the recovery of business processes or IT systems they own/administer.

Table A-1: Level 3 standardized terminology used for communications

Level 3 has chosen LDRPS (Living Disaster Recovery Planning System) by Strohl Systems as the standardized business continuity planning tool to build and maintain business continuity plans. The system is available to those with an LDRPS user account through the Level 3 intranet and enables business units to develop and maintain their plans. ***Figure A-3***, demonstrates the functionalities available on the website.



Find Vulnerabilities

Conduct a BIA to learn how a business disruption could harm your operations.

Build Plans

Enter information about what your plan needs to do, who's going to do it, and the resources they need.

Print Plans

If the time to recover is now, come here to see your plans, print them, and track their status as you recover.

Name Plans

Build a plan structure for your organization.

Customize

Translate LDRPS and add/revise fields on screens.

Administration

Backup and maintain your LDRPS Database.

Security

Decide who can use LDRPS and what they'll see.

Figure A-3: Business Continuity Program Repository

2. 4 BUSINESS CONTINUITY CAPABILITY

2.4.1 Concept of Operations: Disaster Triggers, Response Condition Levels, and ERT Activation

Overview: There are three categories of response to an event: Response Condition 1, 2, and 3, with Response Condition 1 being the most critical. The Level 3 Network Operations Center (NOC), including the Atlanta Operations Center (AOC), has the responsibility of monitoring internal and external events that might call for initiating a Response Condition. Should an event occur that falls within the Response Condition parameters, the NOC leadership team will notify the Event Manager and/or activate the ERT/EIMT with the appropriate Response Condition.

The primary method of ERT/EIMT and CET notification or activation is by means of pager using the TelAlert system. This is a fully redundant system that has the capability to page out first via the Internet and then fail-over to a Public Switched Telephone Network (PSTN) dialer if necessary. Once notified, ERT/EIMT members have a pre-determined period of time to respond, either in person at their designated meet point or via the audio conference bridge. In the event that a primary ERT/EIMT member is unable to respond, the designated successor will automatically be paged. Each ERT/EIMT member has at least two predefined successors.

Once activated, the EIMT will virtually assemble via Conference Bridge, and the ERT will assemble in its designated tactical room. The NOC Situation Room in Building 1000 at the Level 3 Interlocken campus headquarters is the primary Command Center and the location where the BCP sub-teams convene. A separate tactical room has been established at the Interlocken campus for each of the other sub-teams. Dedicated audio conference bridges and video conferencing units are the primary means of internal ERT communications. External Level 3 resources may be directed to join the ERT via the audio conference bridges to provide critical information to the team and to help the ERT effectively manage the event.

2.4.1 ERT Activation Process

When necessary, the Transport Network Operations Center (TNOC) notifies the Event Manager of emerging situations. The TNOC then receives event inputs from a variety of sources, including Global Field Services, the Security Operations Center (SOC), media (e.g., CNN), the EIMT, etc. The TNOC follows documented guidelines that detail when to notify the Event Manager; ultimately, any natural or man-made event that could significantly disrupt the network and/or business processes of the company. The following are just a few of the types of events that necessitate the Event Manager notification: hurricane warnings, Department of Homeland Security

(DHS) “Code Red,” major power outage, network outage, and serious injury or loss of life.

The Event Manager makes the decision to activate the ERT, and, at the Event Manager’s direction, the TNOC initiates a TelAlert page to the ERT. The Event Manager determines who is paged depending upon the severity of the emergency or event. The leads then direct whether sub-teams are paged, if it is appropriate for the event. When summoned, ERT members will either gather in their pre-assigned meeting locations or join their respective conference bridge.

After the initial briefing on the situation, the Event Manager or team leads can then dismiss any ERT sub-teams and/or members not needed for that particular event. The ERT, with primary responsibility and two designated backups, can operate 24 x 7 until the event is resolved. Once the situation or recovery is under control such that it can be managed through standard operating processes, the Event Manager will deactivate the ERT.

2.4.2 Evacuation and Assessment: Facility managers are responsible for ensuring that evacuation plans are developed, documented, and tested to protect the people working within a facility. These plans, at a minimum, contain evacuation procedures, processes for notifying and coordinating with public emergency management (police, fire, medical) organizations, details on conducting an immediate assessment of damage, and notifying higher management of the disaster.

2.4.3 Emergency Management Teams: The ERT/EIMT is composed of the five core sub-teams, which include Corporate BCP, Human Resources, Global Network Services, Metro Network Services, and Corporate Communications. Secondary sub-teams include Information Technology, Corporate Facilities Management, Security, and Europe Operations. Sub-teams may themselves be comprised of smaller groups, organized, called out, and managed by the sub-team itself. Each sub-team is responsible for developing, documenting, maintaining, and employing its own plans necessary to meet its Business Continuity Planning responsibilities.

The cross-functional ERT/EIMT is the primary mechanism to centrally manage and coordinate a significant business disruption. The team is structured to follow the Incident Command model for emergency management advocated by the Federal Emergency Management Agency (FEMA) and Disaster Recovery Institute International (DRII). The ERT/EIMT is activated when internal or external events pose an extraordinary risk that could affect the safety of people, the network, or business assets. Activation is at the discretion of the Event Manager and warranted when an event is out of the ordinary and of sufficient magnitude to require a coordinated response across the enterprise. All critical business units, functional, and corporate groups are represented on the ERT/EIMT and are expected to be available 24 x 7. Each primary member has two designated backups, and primaries are responsible for ensuring a backup is available if they are unavailable.

The primary means of ERT/EIMT activation is through the TelAlert paging system, which is directed by the Event Manager and executed by the TNOC. As a redundant system to TelAlert, members can be paged through the Internet, with a fail-over to PSTN. The page out of the ERT/EIMT can be initiated by the ERT/EIMT communications manager or others if the TNOC is unavailable. Primary ERT members have 15 minutes to accept or reject the TelAlert page. If the primary fails to respond or rejects the page, the page automatically rolls to the successor. Because pagers are not used by Level 3 in Europe, these members receive their TelAlert page through cell phones. Once notified, ERT/EIMT members immediately meet in their designated tactical room or join their sub-team's conference bridge. Each ERT/EIMT member receives a card noting the location of their sub-team's tactical room and the primary and secondary teleconferencing bridges their sub-team uses.

If an event affects the Broomfield, Colorado, campus and incapacitates the members of the primary ERT/EIMT, a backup ERT/EIMT, which follows the same structure and uses the same teleconferencing bridges as the primary, is organized and staffed in Atlanta at the AOC.

The ERT/EIMT members are responsible for the overall direction, sub-team coordination, and final decision making should the ERT/EIMT be activated. The ERT/EIMT has authority to commit enterprise resources as needed, up to $25 million, to ensure life safety, maintain or restore service for customers, protect corporate assets, recover disrupted business and IT processes and systems, and preserve the reputation of the business. Impacts over $25 million or that meet the specific criteria outlined in this plan require coordination and direction from the Corporate Executive Team (CET).

2.4.4 Corporate BCP: The Corporate BCP sub-team facilitates meetings and resources surrounding the event. They have responsibility for support of the ERT/EIMT group, and they capture and disseminate information to the team.

2.4.5 Human Resources: The Human Resources (HR) sub-team verifies EO safety, assesses issues relating to the well-being of EO's, handles employee relations, and interprets HR and related policies.

2.4.6 Global Network Services: The Global Network Services (GNS) sub-team assesses impacts to the facility, customer, and business and implements appropriate strategies and plans.

2.4.7 Metro Network Services: The Metro Network Services (MNS) sub-team assesses impacts to the facility, customer, and business and implements appropriate strategies and plans.

2.4.8 Corporate Communications: The Corporate Communications (CC) sub-team manages potential damage to the company’s reputation, supports media relations, and supports customer communications.

2.4.9 Information Technology: The Information Technology (IT) sub-team assesses technology impacts and restores the technology environment, including all platforms.

2.4.10 Corporate Facilities Management: The Corporate Facilities Management sub-team assesses impacts to non-technical facilities. They assist with implementation of evacuation plan activation and communicate with property management.

2.4.11 Security: The Security sub-team serves as the liaison to the responding public safety agencies. They coordinate interim physical security solutions and initiate investigations as to the cause of the incident.

2.4.12 Europe Operations: The Europe Operations sub-team is responsible for all of the items listed above for each sub-team.

2.4.13 CET Management: This group is composed of the President and COO, CEO, Chief Legal Officer, and the Vice Chairman. They assume that the ERT/EIMT is engaged in managing the event, and all business units are represented. The primary role of the CET is to consider the implications of an event to the company at a level above business continuity/crisis resolution and to respond accordingly. The Event Manager will attempt to coordinate only with the scheduled on-call representative of the CET. This group will handle issues escalated to the Global Vice President (GVP) by the Event Manager to include:

- Situations that threaten to result in the health or safety or result in loss of life of one or more people.
- Situations that threaten or have resulted in a material impact to the business.

- Major property loss or damage.
- Specific and credible criminal or terrorist threats to the business.
- Significant requests for assistance from the National Coordinating Center Command Authorities.
- Situations requiring an immediate expenditure in excess of $25 million.
- Situations that have drawn or are likely to draw significant interest from the national or local media.
- Situations that will have a significant impact on a Top 10 customer.

2.4.14 CET Process: The CET Coordinator will publish a weekly CET schedule to the Executive Administrators (EAs). To the extent that a CET member is unavailable, the Secondary will become the Primary; the Tertiary will become the Secondary, and so on. The CET Coordinator will notify the other CET members and Event Managers. The contact information for the CET is maintained in a secure folder on a shared server managed by the CET Coordinator. Each Thursday, the CET contact information for the following week is updated by the EAs, which the CET Coordinator distributes via e-mail. Contact information for the CET that changes during the current week will be updated by the EAs or the CET Coordinator. Event Managers will refer to the shared file for the most current contact information. The CET, EAs, and Event Managers will be provided with wallet cards containing:

- Current CET, EA, and Event Manager contact information.
- CET's role if an event requires escalation.

If time permits, the Event Managers will wait approximately 20 minutes for a CET member to respond before contacting the next member in the succession order.

2.4.15 CET Coordination Points:

- What is the nature and scope of the business disruption?
- What is the safety status of Level 3 EO's and/or others at the affected location?
- What steps have been taken to address the situation?
- What is the best estimate for service resumption?
- What is the media potential and the ERT's recommendations for media management?
- Has coordination with any Government agencies taken place? Is it necessary?
- Does the ERT have the resources it needs to manage the event?
- When will the next ERT update be provided?

Considerations for action if appropriate for the event:

- Coordinate the information received with other members of the CET.
- Contact appropriate members of the Board.
- Ensure that the media situation has been appropriately addressed.
- Ensure coordination with key financial stakeholders, key customers, and key Government clients and agencies.
- Will the event have an affect on pending Mergers and Acquisitions, and what steps should be taken?
- Could the event affect developing major deals, and should steps be taken?

2.4.16 Recovery: Recovery of disrupted business processes and IT systems is the responsibility of the process owner or the system administrator for a given IT application. Process/IT system owners are required to develop and document a recovery plan in LDRPS that addresses business process/IT system identification, interdependencies, RTOs, necessary resources, recovery teams, and specific recovery tasks. Data needed to develop effective, coordinated, and prioritized recovery plans is gathered through a corporate business impact analysis (BIA). Continuity plans are written from a worst-case standpoint and adjusted to address particular impact situations. Plans are kept up-to-date and reviewed and tested at least annually.

2.4.16 Logistics - Alternate Locations and Capabilities: Level 3 operates backup facilities that are separated geographically by over 1,100 miles to maintain key business processes and capabilities.

2.4.17 Failover Site: A backup data center is located in Atlanta. Critical applications and data files have been identified and continuity strategies relying on this Atlanta facility been developed. Level 3 keeps one complete set of backups, both full and incremental, at a commercial vendor's vault located a safe distance from the data center. The vendor picks up backups daily. The backup tapes are used during continuity exercises to recover the operating systems, production data, and databases, and to restore Local Area Networks (LANs). In addition to the data center plan, alternate recovery strategies have been developed for specialized operations functions located within the IT environment.

Should the Broomfield-based ERT/EIMT become incapacitated, a backup ERT/EIMT is located in Atlanta. The backup ERT/EIMT is fully capable of managing disaster events and participates in regular BCP exercises.

2.4.18 Monitoring: The AOC serves as a second Level 3 NOC. They operate simultaneously and provide 24 x 7 capability to ensure management and control over the Level 3 network.

2.4.19 Technical Customer Account Manager and Customer Network Operations Center: During a Level 3 catastrophic event, the Technical Customer Account Managers (TCAMs) will be dedicated to addressing customer issues. In addition, TCAMs are also located in both network operations centers on a full-time basis to ensure availability.

2.4.20 Facilities: Level 3 maintains over 900 facilities, which affords the resources for use as backup locations when appropriate. Additional backup facilities will be secured as needed by Global Real Estate under the direction of the ERT/EIMT.

2.4.21 Strategic Partnerships: Level 3 will continue to ensure through its vendor management process that all suppliers and partners on which key Government services depend have in place adequate and viable business continuity plans and strategies.

2.5 National Policy-Based Requirements (C.6, C.6.9, C.6.3, C.6.6)

The Level 3 Team deals with network protection and continued service concerns as part of our daily operations. We address these issues for all our customers in our business continuity and disaster recovery planning activities. This section of the proposal addresses network protection and continuation of services for WITS 3 customers.

2.5.1 Basic Functional Requirements (C.6)

In accordance with Executive Order 12472, issued by the National Communications System (NC), Level 3 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 the national telecommunications infrastructure. Therefore, the importance of NS/EP is of an obvious and critical nature.

Level 3 addresses NS/EP within our Business Continuity and Disaster Recovery (BCDR) plans. In this section we discuss how the basic 14 functional requirements in RFP Section C.5.2.1 are met by Level 3.

2.5.1.1 Enhanced Priority Treatment

Voice and data services supporting NS/EP missions should be accorded preferential treatment over other traffic.

Level 3 will ensure that the priority interval prescribed by the agency will be met. Level 3 follows given intervals for Routine, Class B expedited orders and Telecommunications Service Priority (TSP) orders. The provisioning guardrails put in place by Level 3 are monitored by three groups ensuring that each interval is met. Those three groups are Customer Program Manager (CPM), Service Activation (SA), and Project Manager (PM). By utilizing the automation inherent in Level 3's critical-date-management tool, each group can manage to the requested date. This tool also provides Level 3 access into our subcontractors' progress. Using this automation, Level 3 can manage all contractors with real-time responses, eliminating the wait time to gather vital information in completing each order

Our Trouble and Complaint Handling processes are also built to handle TSP services, based on the assigned restoration priority. Services that have a TSP restoration priority that are alarmed issue an automatic page out to the Technical Customer Account Manager (TCAM). 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 current trouble tickets for resolution.

Within the three applicable Level 3 services, various levels of prioritization and protection are available, depending on the service. For example, 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, recent disasters such as hurricanes have taken thousands of time division multiplex (TDM) public switched telephone network (PSTN) users out of service, while VoIP lines that routed traffic via IP backbones remained intact.

2.5.2 National Security and Emergency Preparedness Functional Requirements Implementation Plan (C.6.9, C.6.6)

Level 3 plans for uninterrupted service to our customers in the event of a variety of hazards. This all-hazard approach to network design and operation covers both man-made and natural disasters including intentional attacks and "acts of God." Our continuity of service planning puts Level 3 in a solid position to support WITS 3 customers with continued service even in times of national emergency.

This section contains Level 3's National Security and Emergency Preparedness (NS/EP) Functional Requirements Implementation Plan (FRIP) required by RFP Section C.6.9. Accordingly, our Plan is organized into two parts: Part A addresses the technical systems, administration, management and operational areas proposed to support the basic NS/EP functional requirements; Part B addresses assured service in the National Capital Region as discussed in RFP Section C.6.9. The contents of this plan augment the information contained elsewhere in this proposal.

Individual WITS 3 task orders from a Government agency may have unique NS/EP features or requirements. This plan will be revised or supplemented to address the specific requirements of end-user agencies. This FRIP covers implementation of NS/EP requirements in general for the WITS 3 program.

2.5.2.1 PART A: BASIC FUNCTIONAL REQUIREMENTS SUPPORT

Delivery of Level 3 services occurs over our optic fiber network. Therefore, activities related to protection, monitoring, and restoration of the operation of our network backbone apply to all our services.

Our network architecture and design positions Level 3 to provide WITS 3 customers with IP-based communications in NS/EP scenarios. Agencies have the option of specifying various levels of priority for restorations of service and packet delivery. Our system supports all private addressing schemes as well as encryption options for identity protection. Our services are available nationwide and receive and transmit traffic to international locations.

Implementation of some of the functional requirements is best handled with multiple design features or actions. This FRIP covers the specific actions Level 3 has taken, or features or functions Level 3 has in place, to provide the following functional requirements:

- Secure Networks
- Restorability
- Survivability/Endurability
- Reliability/Availability

Level 3 participates in the Department of Homeland Security's National Coordination Center for Telecommunication (NCC) activities. We have a primary and alternate representative available 24x7.

2.5.2.1.1 Technical Systems

This section of the FRIP describes the technical systems and passive design features that protect the Level 3 Network ensuring our ability to provide services to WITS 3 customers.

2.5.2.1.1.1 Fiber Protection

The vast majority (well over 99 percent) of Level 3 built fiber is deeply buried at least 48 inches underground. Where this depth is not possible, other protection methods are utilized (e.g., bridge attachments).

2.5.2.1.1.2 Earthquake Preparedness

Level 3 complies with local and national earthquake codes and standard practices in all seismically classified geographic areas for our infrastructure and collocation facilities. Features of these facilities include, but are not limited to, the following:

- Seismic bracing for the raised floor
- Seismic bracing for cabinets
- Seismic bracing for electrical switchboards
- Seismic bracing for overhead distribution trays and troughs
- Seismic bracing on the piping and associated supports
- Redundant DC power plants that are also seismically braced
- Compliance with OSHA standards in all facilities

2.5.2.1.1.3 Facility Protection

Facility protection is provided through uninterruptible power sources (UPSs), DC systems, battery backup for non-critical systems, and automatic transfers switches (ATS).

UPSs are provisioned in an N+1 configuration and range in size from 125kVA to 1000kVA with 480 VAC, 3-phase input and output. The UPSs support all customer AC equipment.

Each UPS battery system is designed to carry full load for 15 minutes without a generator. Emergency generators typically provide back-up power in less than 10 seconds and are sized to support the entire facility at maximum load. The generator is configured for auto-start upon utility power failure. The emergency generator has enough fuel to support more than 24 hours of autonomy at maximum load. The fuel delivery company is notified as soon as the generator fires up, which allows them to schedule regular deliveries in the event that power is not restored within 24 hours.

Refueling is scheduled to occur when the tank reaches approximately 50 percent of its capacity.

The DC power backup time is four hours at 100 percent load. The DC plant supports all customer equipment and critical Level 3 equipment.

Battery backup for emergency lighting is provided on approximately 10 to 15 percent of lights, according to building code. In the event of a power failure, the emergency lights will continue to operate. Once the generator starts up, all lights and all non-critical equipment in the facility will regain power and become fully operational.

The ATS is the device that monitors utility power, controls generator operation, and connects the generator to the facility switchboard in the event of a utility failure. When the ATS determines that the utility power is absent or out of specification, it starts the generator. Once the ATS determines that the generator is at the appropriate voltage and frequency, it connects the generator to the Facility switchboard, which restores power to all systems within the facility. Level 3 has purchased a maintenance bypass option that allows maintenance of the ATS without service interruption. To minimize main feeder lengths, the ATS units are located as close as possible to the generator and utility service entrance.

2.5.2.1.1.4 Fire Detection and Suppression Systems - Sprinkler Design Approach

The fire protection sprinkler system is a double interlocked pre-action system designed to provide the best security against accidental discharge of water from the sprinklers. The pre-action system interfaces with a fire alarm system. Under normal conditions, the overhead sprinkler piping contains compressed air. When the smoke detector is activated, the pre-action valve opens to fill the overhead piping with water and sends a signal to the fire alarm panel. Water will discharge only from the sprinklers that have been subject to enough heat to melt the fusible link on the water head. This fusible link is the second interlock in the system.

2.5.2.1.1.5 Network Security

The Level 3 security architecture was designed to detect unauthorized devices in our commercial and internal networks. An inventory of all network attached devices is updated daily by automated systems. The inventory data is analyzed by automated processes to identify rogue systems. Integrity checking for all network attached resources is performed daily. The results of the inventory analysis are logged for reporting. If necessary, alerts are generated for problem resolution.

Level 3 is particularly aware of the potential for Denial of Service due to malicious attack. Through continuous network monitoring, Level 3 detects and responds to problems immediately, whatever their cause. Our network architecture is equipped to detect service-affecting intrusions and can apply controls specifically designed to mitigate hostile traffic.

The entire Level 3 Network runs over optic fiber over which makes it more difficult to access or tap into than signals transmitted over copper cable. The Level 3 cable is terrestrial and the vast majority of it is installed within duct at a minimum burial of 48 inches. Warning tape lies above all duct banks and fiber maintenance chambers are concrete boxes with secure 100-pound metal lids. A second layer of security is provided in metro areas with a special locking mechanism called a manhole barrier (made from 15-gauge stainless steel requiring special keyed tools to gain access). Routes are continuously monitored by Level 3's Network Operations Center (NOC) as well as physically by our field operations staff.

2.5.2.1.1.6 Rerouting and Redundancy

The Level 3 Network was designed to be completely redundant and resilient. No single point of failure exists in the backbone and a redundant hardware path is always available in the event of equipment or circuit failure.

Within the supporting transport network, we plan for 100 percent restoration of a worst-case single fiber cut. In our gateways, planned capacity considers full redundancy in the case of a single router failure.

Level 3 uses MPLS as the base redundancy mechanism. Each top-level node in the Level 3 Network is connected to two or more other top-level nodes via unprotected 10 Gbps wavelengths. If any wavelength goes down, MPLS automatically re-routes traffic around this failure. In addition, OSPF and BGP protocols running on the backbone ensure that traffic continues to be routed if a failure occurs.

2.5.2.1.2 Administration

When services are purchased, the Government agency customer has the opportunity to request Telecommunications Service Priority (TSP) restoration. The customer can specify the category of priority provisioning and restoration for the services they are purchasing. Category E is available for Emergency priority. The Level 3 TSP priority sequence follows the Executive Order-required sequence.

2.5.2.1.2.1 Security Personnel

The Level 3 security personnel are trained to address all types of security risks, safety issues, business continuity, and disaster recovery. Groups under this umbrella include Data Privacy, Network Security Architecture and Engineering, Network Security Operations, Investigations, Policy and Plans, Business Continuity/Disaster Recovery, Physical Security, Government Security, and Field Security in North America and Europe.

2.5.2.1.2.2 Security Assistance to Customers

Level 3 is committed to providing security assistance to customers and those beyond the Level 3 Network, such as helping trace problems, and addressing sources of and solutions for those problems.

2.5.2.1.2.3 Network Security Measures

Level 3 provides tracking systems to trace distributed Denial of Service and other such attacks to their sources at the edge of our network. We collaborate with industry-leading managed security service providers and support legally authorized governmental efforts to trace and identify sources of criminal acts.

2.5.2.1.2.4 Professional Outreach

Level 3 is a member of the Association of Contingency Planners (ACP) and Disaster Recovery Institute (DRI) International. Level 3 is also a member of several industry forums that deal specifically with security assessment functions such as the High Tech Crime Investigation Association, the Computer Security Institute, the American Society for Industrial Security Cyber Crimes & Threats Task Force, and the International Association of Chiefs of Police Private Sector Liaison Committee. The firm is also a charter member of the Internet Services Provider (ISP) Security Consortium.

2.5.2.1.2.5 Data Privacy

Level 3 was the first telecommunications corporation to receive “Safe Harbor” status from the U.S. Department of Commerce.

All critical applications and data files have documented manual workaround procedures. One complete set of back-ups, both full and incremental, are stored at a vault located a safe distance from the data center.

Level 3, whose network is an acknowledged component of the nation's telecommunications critical infrastructure, has formed a close partnership with the Federal Government to put processes in place to fully coordinate looming or actual disasters in order to minimize the impact to network assets and services. To further build ties with Government emergency management programs, Level 3 is an active participant in the National Communications System's National Coordinating Center (NCC) for Telecommunications. The company will maintain a representative and an alternate to the NCC who will regularly participate in national-level coordination meetings, regional exercises, and actual disaster response events to build an effective partnership for responding to emergencies. Disruptive events that affect Government customers will be immediately communicated to the NCC through Level 3's NCC Coordinator.

2.5.2.1.2.6 Coordination Requirements

Upon notification that a disaster event either has or is about to occur that has the potential to disrupt network services for Government customers, the Emergency Response Team (ERT) will immediately begin proper coordination with the Government. The Government Operations representative to the ERT will be responsible for monitoring all disaster events for the need to initiate such coordination.

2.5.2.1.2.7 Notification and Liaison

Should a disaster have major consequences on WITS 3 services, the WITS 3 PMO will be notified immediately, but not later than 15 minutes after such determination, by the Government Operations representative on the ERT through communication channels established following contract award. Following the initial notification, the ERT will dispatch the pre-assigned WITS 3 Liaison to meet and work with the PMO until the disruption is resolved.

The Liaison, who will be a different individual from the NCC Coordinator, will be on site with the PMO no later that four hours after the disruption is identified and will maintain direct contact back to the ERT. In addition, the Government Operations members of the ERT will pre-identify WITS 3 suppliers, partners, and other stakeholders who need to be notified at the onset of a disaster and coordinated with throughout the event. Requirements for WITS 3 WITS 3 Liaison personnel are as follows:

- Shall be cleared at SECRET level or higher
- Shall be different from the NCC coordinator
- Shall be dedicated during a disaster to working only WITS 3 issues
- Shall be prepared to discuss classified requirements at the planning and operational levels
- Shall be formally named in the Disaster Recovery Plan
- Shall be familiar with the general and technical management organization of Level 3
- Shall have established channels (through the ERT) for initiating necessary actions and obtaining necessary decisions for disaster recovery
- Shall be on site with the PMO no later than 4 hours after receiving notice of a disaster
- Shall be available, as requested by the PMO, on an extended basis during a disaster event

2.5.2.1.2.8 Prioritization

Given its importance to national security, WITS 3 will be Priority 1 (Essential Functions) for restoration and recovery. Level 3 will manage the recovery of WITS 3 Operations. However, the WITS PMO will identify priorities for WITS services recovery.

2.5.2.1.3 Management

The Level 3 planning for emergency response is well maintained and exercised within the requirements of our Business Continuity and Disaster Recovery Program. Management of the restoration of services and maintaining service functions is generally as described below:

2.5.2.1.3.1 Communications Network

Through the Level 3 NOC, we identify and isolate causes of potential network failure and coordinate resolution of system outages.

2.5.2.1.3.2 Gateways

Each Level 3 Gateway has documented fail-over plans for each system used (e.g., commercial power, HVAC, and UPS). Gateways have evacuation plans with posted evacuation routes.

2.5.2.1.3.3 Interlocken Campus

Each department will follow procedures for maintaining critical business functions during a disaster recovery period. The Plan will also identify business functions to be suspended until normal operations resume, as well as potential business risks and exposures associated with performing under austere conditions dictated by a disaster.

2.5.2.1.3.4 Data Center

All critical applications and data files have been identified, and the Plan documents manual workaround procedures. Level 3 keeps one complete set of back-ups, both full and incremental, at a commercial vendor's vault located a safe distance from the data center. The vendor picks up back-ups daily. The back-up tapes are used during recovery exercises to recover the operating systems, production data, and databases, and to restore Local Area Networks (LANs). In addition to the data center plan, alternate recovery strategies have been developed for specialized operations functions located within the information technology environment. These include the following:

- **Technical Customer Account Manager and Customer Network Operations Center**: During a Level 3 catastrophic event, the Technical Customer Account Manager (TCAM) will be dedicated to addressing collocation customer issues. In addition, TCAMs are also located in the Level 3 NOC on a full-time basis to ensure availability.
- **Plan Repository — Living Disaster Recovery Plan System (LDRPS):** This is Web-based software with an SQL server database purchased for hosting and maintaining all critical information. In addition to full weekly and daily incremental back-ups, a nightly replication of the production database is transmitted to the redundant system in our off-site data center. The information in the database consists of employee names, Level 3 facility information, those requiring emergency notification, call-out and escalation information, decision guidelines, tasks, and checklists. In addition to housing disaster recovery plans, LDRPS also contains plans for business continuity from each business unit.

Should a network disaster be declared, a formalized ERT will be deployed to manage the event. Level 3 already has a Disaster Recovery Plan in place to address such an event or a disaster is declared for the continuance of our business.

The response and notification process includes, but is not limited to, the following steps:

- Transport Network Operations Center (TNOC) notifies Event Manager of emerging situations
    - TNOC receives event inputs from variety of sources, including Global Field Services, the Security Operations Center (SOC), media (e.g., CNN), BCDR Planning Team, etc.
    - TNOC follows documented guidelines for when to notify Event Manager: ultimately, any natural or man-made event which could significantly disrupt the network and/or business processes of the company will result in notification.
    - Types of events necessitating Event Manager notification:
        - Hurricane warnings
        - Department of Homeland Security “Code Red”
        - Major power outage
        - Network outage
        - Serious injury or loss of life
- Event Manager makes decision to form the ERT
- At Event Manager’s direction, TNOC initiates TelAlert page to ERT
    - Event Manager can direct that either just the leads from each sub team be paged or that the entire ERT be paged

  - Leads can then direct that their sub teams be paged if appropriate for the event

- When called out, ERT members will either gather in their pre-assigned sub team meeting locations or join their respective conference bridge
- After initial briefing on the situation, the Event Manager or team leads can dismiss any ERT sub teams/members not needed for that particular event
- ERT, with primary and two designated backups, can operate 24x7 until event is resolved

Once situation/recovery is under control such that it can be managed through standard operating processes, the Event Manager will deactivate the ERT.

The Disaster Recovery Plan will provide for situation assessment, escalation procedures, operational and security response, and media communications. The Level 3 emergency response is well rehearsed, with an active exercise program testing emergency management and recovery several times a year. Exercises are closely monitored by evaluators, strengths and weaknesses are documented, and formal plans are updated to reflect lessons learned.

2.5.2.1.4 Operations

The Level 3 NOC is responsible for all facilities and network management, monitoring, and repair. Level 3 operates three NOCs that monitor the Level 3 Network 24x7. We staff highly trained operations managers and network technicians at regional monitoring centers located in Denver, Atlanta and London.

The Level 3 NOC provides 24x7 surveillance, repair and utilization monitoring of all Level 3 core network layers and technology. The NOC provides proactive monitoring of customer traffic across our network, through which we can identify potential problems and provide resolution before our customers even know there's an issue. Some environmental alarms are monitored both locally and at the NOC, and 100 percent of circuit performance monitoring is done at the NOC.

Two of the NOCs are redundant and separated by 1,500 miles. These NOCs, located in Denver and Atlanta, are staffed with network operation technicians and specialists using an out-of-band network management network system to control routing, prevent outages, restore service, and monitor network security.

The WITS 3 security management functions will be performed at corporate facilities in Herndon, Virginia; Denver, Colorado; and Atlanta, Georgia. At all these locations, Level 3 has in place a robust and complete physical security program that includes centrally monitored environmental controls, fire suppression systems, card-access controls, alarms, Closed Circuit Television (CCTV), and central monitoring and recording of access control systems. External and internal doors are locked and alarmed. Level 3 routers, switches, and other equipment are located in discreet, locked spaces. Access control systems record arrivals of authorized persons; CCTVs run 24x7 at certain locations within the facilities. The CCTVs document activities and enable the staff to monitor individuals and certain activities within the facilities. Certain areas of the facilities are sensitive and require another level of control. Dedicated 24x7 security monitoring technicians respond to all physical alarm events. Additional controls at the Colorado and Georgia locations include guards, power back-up systems with emergency generators, and biometrics. Access to these areas requires authorized personnel to have validated palm scans to gain entry.

Level 3 has documented failover plans for each system (e.g., commercial power, heating, ventilation, and air conditioning [HVAC], and uninterruptible power Supplies [UPS]).

2.5.2.2 Part B: National Capital Region Coverage [C.5.2.7, F.2(93)]

Although Level 3 is committed to reliable, continuous service at all locations, we are aware of the centric nature of Government operations in the National Capital Region — the Washington DC area. This is a highly reliable region in the Level 3 Network, due to the large installed base of redundant fiber routes. Assurance of service requires high reliability, and reliability is a core feature of Level 3's service offerings.

This level of reliability is network-wide, which is important for service assurance in the Washington DC area, because customers there connect to locations throughout the nation. The completed Level 3 terrestrial and transoceanic transport network is fully route-diverse with no single points of failure at the physical level. Level 3 designed its IP backbone using the most direct routes between markets on our transport network. Today we have multiple OC-192 express routes connecting high-traffic areas. This allows us to provide an Internet access product with very low latency, high reliability, and low cost.

Level 3 will offer geographically separate network switches/routers to serve Federal agencies in the National Capital Region. For IP-based services, each customer will have the option of diversity. This includes access diversity, POP diversity, and switch or router diversity where available.

Diversity is not a commercial off-the-shelf offering from any vendor, because depending on the location of the customer in relationship to the vendor's network, it may be straightforward, or extremely difficult. For this reason Level 3 looks at each diversity request on an individual case basis. It is always possible to offer diversity—however in some cases the solution may include significant cost.

Fortunately, most Federal Buildings are located in the downtown area of Washington DC. This area is rich in Level 3 fiber and access points. Level 3 will work with WITS customers to develop Government customer-specific requirements for coverage in the national capital region. A task order specific FRIP will provide the details of service functions and maintaining or restoring services during NS/EP events as needed.

2.5.3 Protection of SS7 Signaling Systems (C.6.3)

The Level 3 VOIPTS service runs on a huge platform extending across the US. The VoIP network hands calls off to the PSTN and vice-versa, which requires high-speed SS7 signaling and protection of such signaling. There are two ways to protect such signaling systems from unauthorized access: encryption and physical isolation.

Level 3 does not use encryption as a means to protect SS7 signaling—primarily because encryption forces the equipment to add delay into the processing of SS7 control packets. Level 3 designed the SS7 network for extremely fast response. Isolation of the network itself and implementing a core component into the STP—the Eagle 5 SAS—has enabled several very successful methods of SS7 protection. The following methods combine to securely protect all SS7 control elements:

- Physical isolation of the SS7 physical network
- Message throttling
- Retransmissions protection
- Controlled rerouting
- Gateway screening

Level 3 uses the Tekelec EAGLE 5 Signaling Application System (SAS) for our Signal Transfer Point (STP), which provides a rich set of SS7 services, with secure protection embedded into the software.

The Eagle SAS delivers the performance levels to drive the Level 3 voice network. From a single platform, the EAGLE 5 SAS provides STP, signaling, application server, and network monitoring functions. Tekelec's EAGLE 5 SAS delivers dramatic increases in database size, signaling capacity, and transaction speed. These advanced features are coupled with next-generation IP connectivity, providing a smooth transition to the new network model being used with our VoIP platform.

The SS7 signaling is carried across Level 3's transport networks. The same physical isolation and security applies here as it does to protection of all data across our backbone. All SS7 links run through fiber-optic cables, which are buried at a depth of 48 inches below ground. In cases where it is impossible to bury the cables, they are protected with sealed, steel-conduit and/or concrete slabs.

At all points where the fiber or copper terminates, the facility is secured by steel doors with locking mechanisms, badge readers, and palm scanners (which are used at all Level 3 Gateways).

The SS7 network has been designed to comply with Level 3's security requirements for physical and remote access.

The SS7 system could conceivably be compromised if an attacker were to cause congestion or a Denial of Service (DOS) condition. This could be done by flooding and/or errant malformed packet generation, or a cleverly disguised series of messages that cause massive rerouting to occur. The Eagle 5 SAS has a series of congestion avoidance routines already in place, such as Message Throttling, Retransmission Protection, and Controlled Rerouting.

2.5.3.1 MESSAGE THROTTLING

To protect SS7, automatic dampeners have been installed to deal with congestion control. For Level 3, this is a standard component of SS7, and our STPs have this feature enabled. We are compliant with SS7 congestion control as defined in Telcordia GR-246-CORE.

Procedures were added to the EAGLE 5 SAS mail transfer protocol (MTP) protocol to control STP signaling message congestion handling. If the STP has an internal failure that causes a reduction in the STP's signaling message handling capacity, an option exists for the EAGLE 5 SAS to request traffic to be rerouted by sending TFR messages to adjacent SPs with the destinations of discarded messages indicated. This also includes provisions for the discard of messages by priority.

2.5.3.2 RETRANSMISSION PROTECTION

If a link has a large number of retransmissions, the traffic of the link could increase enough to cause congestion on that link. To correct this condition, EAGLE 5 SAS will start a T31 timer whenever a link goes into congestion. If the link remains in the same congestion state until T31 expires, the link will be removed from service. The link will become unaligned; then the alignment procedure will be started.

The congestion level that starts the T31 timer is also provision-able to either congestion level 1 or congestion level 2. T31 is started for a link anytime it reaches this congestion level or a higher level. An increase in congestion level or an abatement to a lower congestion level restarts the timer. Abatement to below the provisioned congestion level stops the timer. For example, if T31 is 60 seconds and a link goes into congestion level 1, a 60 second T31 timer is started. If after 45 seconds the link's congestion increases to level 2, the timer is restarted. If the link remains at congestion level for 60 seconds, the link is taken out of service.

2.5.3.3 CONTROLLED REROUTING – PROTECTION AGAINST EXCESSIVE REROUTES

This procedure eliminates the possibility of congestion resulting from a burst of rerouted traffic emanating from the failure of other signaling routes by pacing the broadcast of TFx/ TCx messages. This regulation of broadcast has the net effect of dealing with congestion much more effectively.

Controlled rerouting is performed by a signaling point upon receipt of a transfer-allowed or transfer-restricted message, which results in traffic being diverted from a less-efficient route to a more-efficient route. During controlled rerouting, the signaling point stops traffic toward a specific destination on the current route. It then buffers messages for a prescribed time period before routing them on the new route. This is done to minimize message mis-sequencing by allowing time for the traffic already on the less-efficient route to reach its destination. After the EAGLE 5 SAS broadcasts TFA/TCA or TFR/TCR messages announcing the change in status, multiple signaling points may perform controlled rerouting and release messages on the new route nearly simultaneously. This burst of rerouted traffic is a potential source of congestion. This is available for both ANSI and ITU networks. If TFA/TFRs are sent for affected X.25 pseudo point codes, they are also paced.

2.5.3.4 GATEWAY SCREENING

In addition to message throttling, Level 3 has implemented gateway screening on the SS7 network at all PSTN interconnection points. Gateway screening is similar to that of a firewall in the IP world, only it filters traffic into the SS7 STPs.

Gateway Screening (GWS) is used at gateway STPs to limit access into the network to authorized users. A gateway STP performs inter-network routing and gateway screening functions. The GWS is provided on the EAGLE 5 SAS to control access to non-home SS7 networks. The feature includes both inbound and outbound message screening.

The EAGLE 5 SAS's implementation of GWS adheres to the requirements stated in GR-82-CORE. The EAGLE 5 SAS's current implementation of gateway screening supports this process on as many as 255 linksets, and each linkset can be allowed one of 255 screen sets. Each screen set can contain up to 4,000 entries (rules). There are no translation table limits or interdependencies among these screening tables. To support rapid access and download following a processor restart, all GWS tables are also stored on at least two dedicated GLS (Generic Loading Service) cards.

Gateway screening provides two levels of screening, MTP and SCCP—as depicted in ***Figure A-4***.

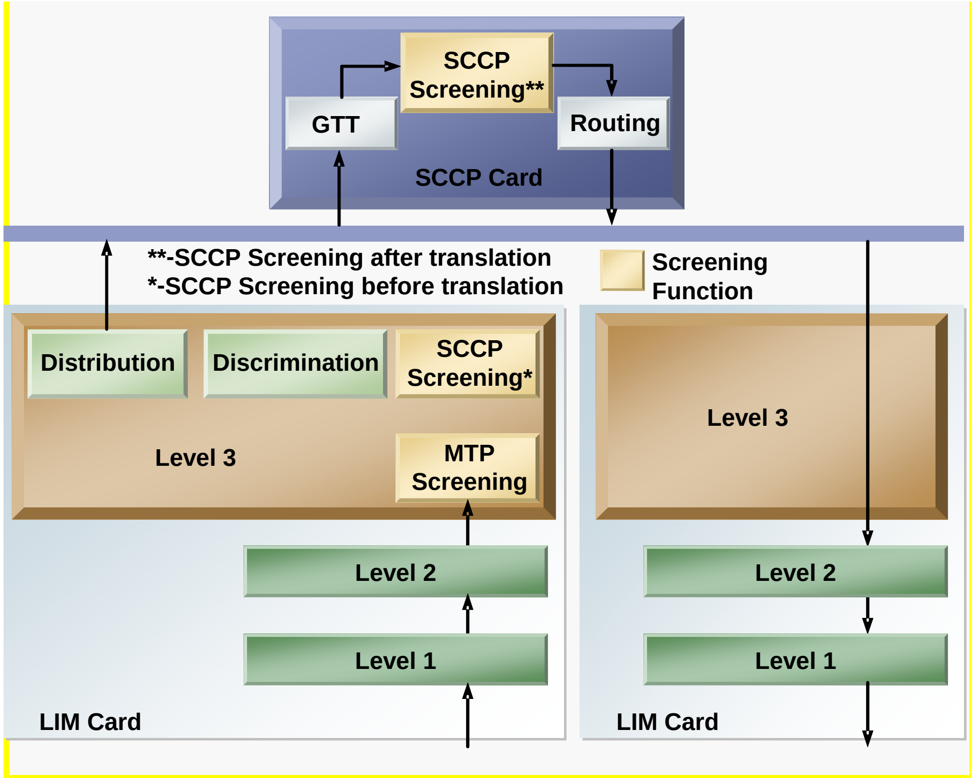


Figure A-4: Gateway Screening Functional Diagram

MTP screening enables the user to screen based on the following:

- Allowed OPC (OPC)
- Blocked OPC (BLKOPC)
- Allowed SIO (SIO)
- Allowed ISUP Message Type (ISUP)
- Allowed TUP Message Type (TUP)

- Allowed DPC (DPC)
- Blocked DPC (BLKDPC)
- Allowed priority values per SI value
- Allowed HO-HI fields (SI=0,1,2)
- Affected destination field for network management

SCCP screening allows the user to screen based on the following:

- Allowed Calling Party Address (CgPA)
- Allowed Translation Type (TT)
- Allowed Called Party Address (CdPA)

2.5.4 Assured Service in the National Capital Region (C.6.3)

Although Level 3 is committed to reliable, continuous service at all locations, we are aware of the centric nature of Government operations in the National Capital Region—the Washington, DC area. This is a highly reliable region in The Level 3 Network due to the large installed base of redundant fiber routes. Assurance of service requires high reliability, and reliability is a core feature of Level 3's service offerings.

This level of reliability is network-wide, which is important for service assurance in the Washington DC area, because customers there connect to locations throughout the nation and the world. The completed Level 3 terrestrial and transoceanic transport network is fully route-diverse with no single points of failure at the physical level. Level 3 designed its IP backbone using the most direct routes between markets on our transport network. Today, we have multiple OC-192 express routes connecting high-traffic areas. This allows us to provide an Internet access product with very low latency, high reliability, and low cost.

Level 3 will offer geographically separate network switches and routers to serve Federal agencies in the National Capital Region. For IP-based services, each customer will have the option of diversity. This enables includes access diversity, POP diversity, and switch or router diversity where available.

Diversity is simply not a COTS offering from any vendor, because depending on the location of the customer in relationship to the vendor’s network, it may be straightforward or extremely difficult. For this reason, Level 3 looks at each diversity request on an ICB (Individual Case Basis). It is always possible to offer diversity; however, in some cases, the solution may include significant cost.

Fortunately, most Federal Buildings are located in the downtown area of Washington, DC. This area is rich in Level 3 fiber and access points, as shown in ***Figure A-5***. For example, a Federal customer can order two access circuits to two different Internet access edge routers, one in McLean, VA, and another in Baltimore, MD.

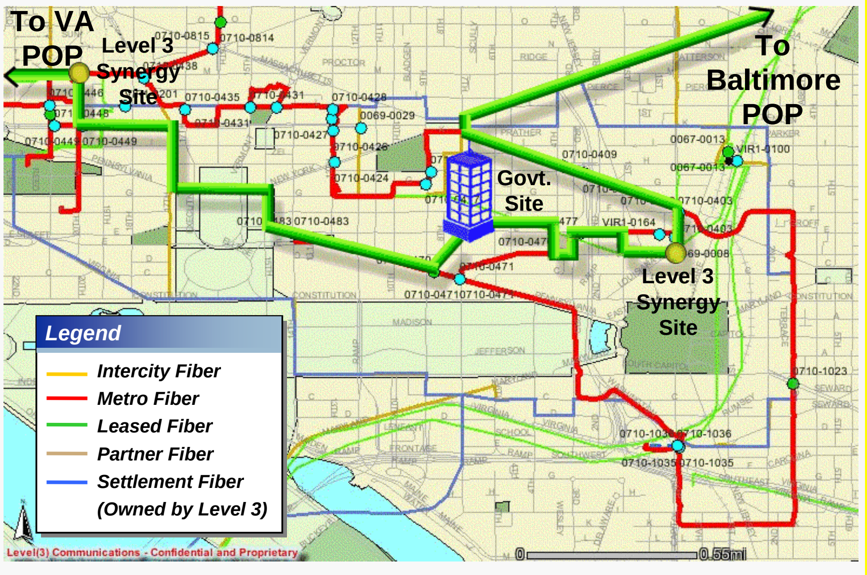
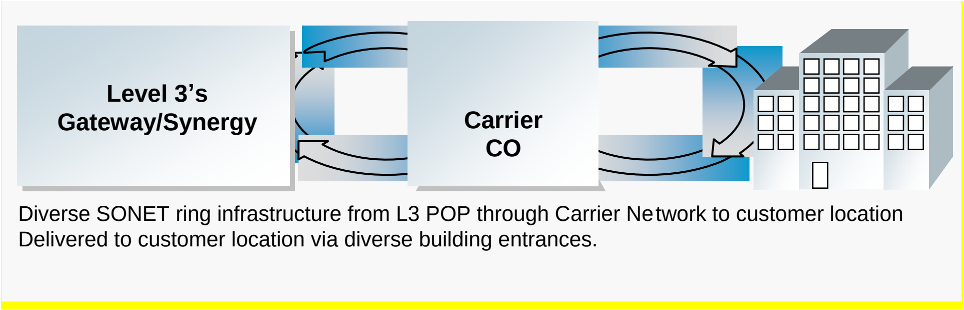


Figure A-5: Map of Downtown Washington, DC

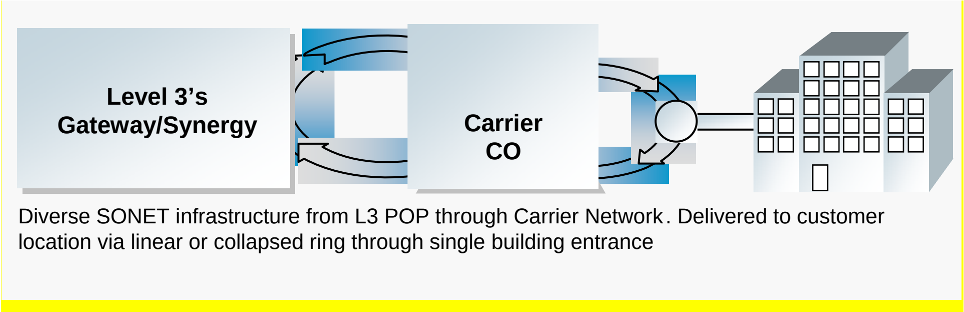
Not only does this arrangement allow for load sharing if desired, it also includes an increased availability service level agreement (SLA).

Figures A-6 through A-9 display several diversity arrangements that might be used:



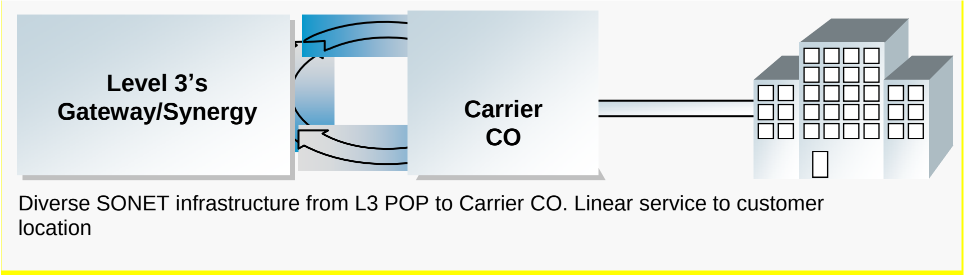
Diverse SONET ring infrastructure from L3 POP through Carrier Network to customer location Delivered to customer location via diverse building entrances.

Figure A-6: Fully diverse to customer premises



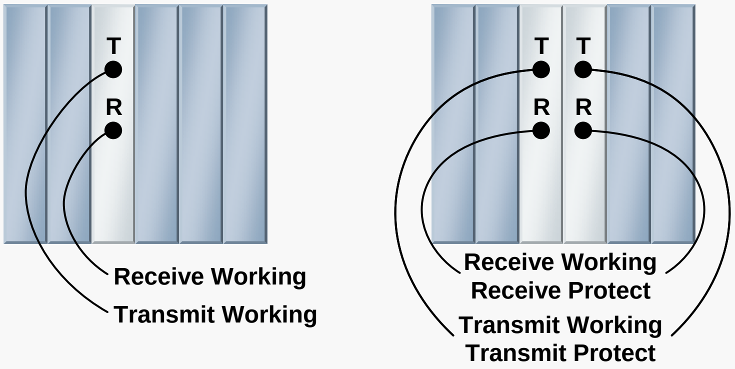
Diverse SONET infrastructure from L3 POP through Carrier Network. Delivered to customer location via linear or collapsed ring through single building entrance

Figure A-7: Fully diverse to manhole



Diverse SONET infrastructure from L3 POP to Carrier CO. Linear service to customer location

Figure A-8: Diverse to SWC



An unprotected hand-off gives a single working and protect interface. A 1+1 protected hand-off (card protection) provides a redundant transmit and receive interface to protect against a optical or card failure.

Figure A-9: Card Protection Diversity

The number of points available for directly accessing a network is critical to its value, which is directly correlated to the number of other networks or nodes to which it is connected. Additionally, the locations of these access points are key to reaching a critical mass of customers, increasing performance, and lowering costs. The scalability of these access points is critical as the Internet grows and participants' demand increases.

The Level 3 IP platform can be accessed in more than 201 markets internationally via more than 5,700 POPs on the continuously upgradeable Level 3 Network. Our IPS can be offered at any of these on-net points of demarcation.

Level 3 is continually adding new on-net buildings and new points of demarcation (within existing on-net buildings) onto its network. Unlike some competitors, Level 3's built network has robust metro fiber networks in 113 metropolitan areas nationwide, enabling Level 3 to easily add buildings and points of demarcation onto the network.

To meet the RFP Section C.5.2.7 requirement of keeping loss to within 15% of total network traffic if one of two router or switch paths were to go down, the resulting traffic increase on the backup router must be managed. This can be done in the initial design phase, and then later by enforcing build-out requirements. We initiate build-outs whenever the network load of a router exceeds 70% utilization. This means that if ALL traffic from one router were suddenly placed on another, the net effect would be to max the traffic at 140% utilization. It may seem that 40% of the traffic will be lost. However, this is not the case.

Routers do not have a 1:1 relationship. If a Level 3 router or link to that router goes down, the resulting traffic load increase is absorbed across multiple routers. Therefore, an outage of one router or link will result in only a nominal increase of traffic elsewhere. For customers that are dual-home, they will also only suffer a small reduction in traffic delivery, if any.

If a national emergency occurs, it is crucial that services continue unabated. This is where Level 3's Business Continuity and Disaster Recovery (BCDR) plans come into play.

The Level 3 risk management systems include prevention and mitigation solutions. When threats cannot be prevented, such as a backhoe fiber cut, the plans implement mitigation techniques to reduce any exposure to our customers. For example, the Level 3 Network design includes Synchronous Optical Network (SONETS) features that provide automatic traffic rerouting (with an average of 50ms for switching). Also, the Level 3 Network is "fully redundant," which means that all routes have alternate paths for, e.g., the fiber connected to each building enters from at least two completely separate points.

Redundancy and resiliency are critical to the proper operation of any network. Networks should be designed with no single point of failure and should be robust enough to function without impairment when network problems occur. If a problem arises, a provider should have the processes in place to restore the network quickly.

Failure analysis is important because all networks are subject to fiber cuts, equipment outages, and so forth. The degree of analysis of all possible failure scenarios determines how stable a provider's network is, despite these failures. Failure analysis is an important component in ensuring a service level agreement (SLA) for network availability.

The Level 3 Network was designed to be completely redundant and resilient. No single point of failure exists in the backbone, and a redundant hardware path is always available in the event of equipment or circuit failure.

Within the supporting transport network, we plan for 100% restoration of a worst-case single fiber cut. In the gateways, planned capacity considers full redundancy in the case of a single router failure.

Level 3 uses MPLS as the base redundancy mechanism. Each top-level node in The Level 3 Network is connected to two or more other top-level nodes via unprotected 10 Gbps wavelengths. If any wavelength goes down, MPLS automatically re-routes traffic around this failure. In addition, Open Shortest Path First (OSPF) Protocol and Border Gateway Protocol (BGP) running on the backbone ensure that traffic continues to be routed if a failure occurs.

Level 3 designs and upgrades its IP backbone such that when any circuit reaches 50% utilization during the peak busy hour for five days in a row, a circuit is immediately upgraded. This policy enables Level 3 to guarantee availability plus low latency and low packet loss even in worst case failure scenarios.

The Level 3 advanced planning process combines capacity forecasting and real-time network monitoring. The company tracks historical performance and forecasts expected traffic growth. This information is used to plan capacity upgrades and order equipment. Additionally, real-time usage is measured using network utilization statistics to ensure that lit capacity exceeds current customer requirements in both normal and fail-over usage modes.

The network topology involves multiple redundant paths, with self-healing rings. All core equipment such as routers, switches, and ADMs are inventoried with hot-standby units in place. In addition, all facilities are reinforced structures, which are secured with reinforced-steel doors and require access badge and/or a palm scan for entrance to the facility.

To date, through recent acquisitions, Level 3's core network includes 36,000 route miles of Level 3-operated, intercity terrestrial fiber in North America. Additional route miles will become available as integration efforts proceed.   In addition, the Level 3 Network has no network spurs. The North American network alone has an underlying 15-ring infrastructure. ***Figure A-10*** illustrates the ring infrastructure in the Eastern United States. This completed network is optimized end-to-end for IP and is

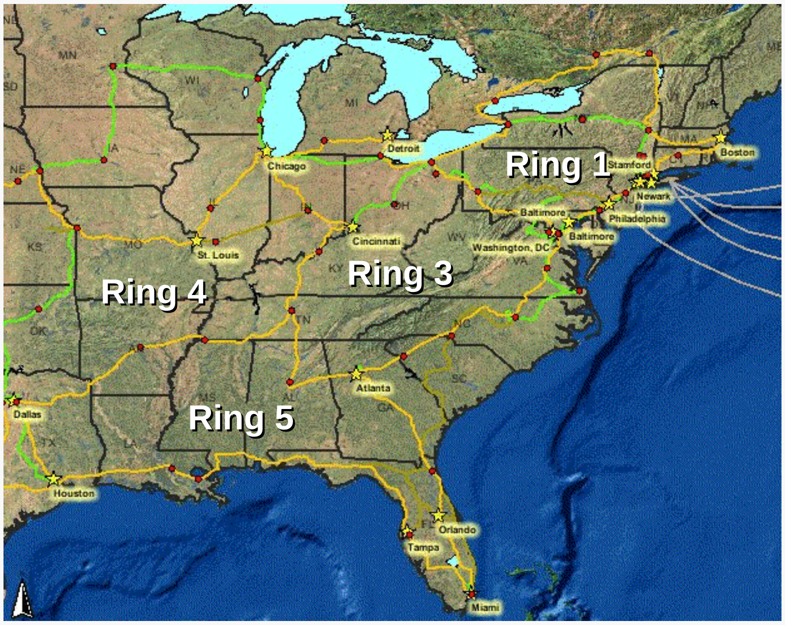


Figure A-10: Overlapping BLSR SONETS rings connecting the National Capital Region to the rest of the United States

operated entirely by Level 3. Hundreds of miles of Corning LEAF (Large Effective Area Fiber), NZ-DSF(Non-Zero Dispersion-Shifted Single-Mode) fiber criss-crosses the entire region, with a secure, redundant ring topology. In regards to the rest of the US, Level 3 has strategically installed numerous BLSR (bi-directional Line-Switched Rings), with a 50 ms restoration time in the event of a fiber cut.

The National Capital Region has three major pipelines connecting it to the other metropolitan areas in the US that act as separate, redundant paths for traffic. Even if one of the three goes down, service remains active as the traffic is rerouted, since each of these pipelines is a part of the nationwide self-healing rings architecture.

Level 3 spent years designing and building the Washington, DC network with the primary goal of redundancy and diversity throughout (see ***Figure A-11***). Two overlapping Unidirectional Path Switched Rings (UPSRs) run throughout the main

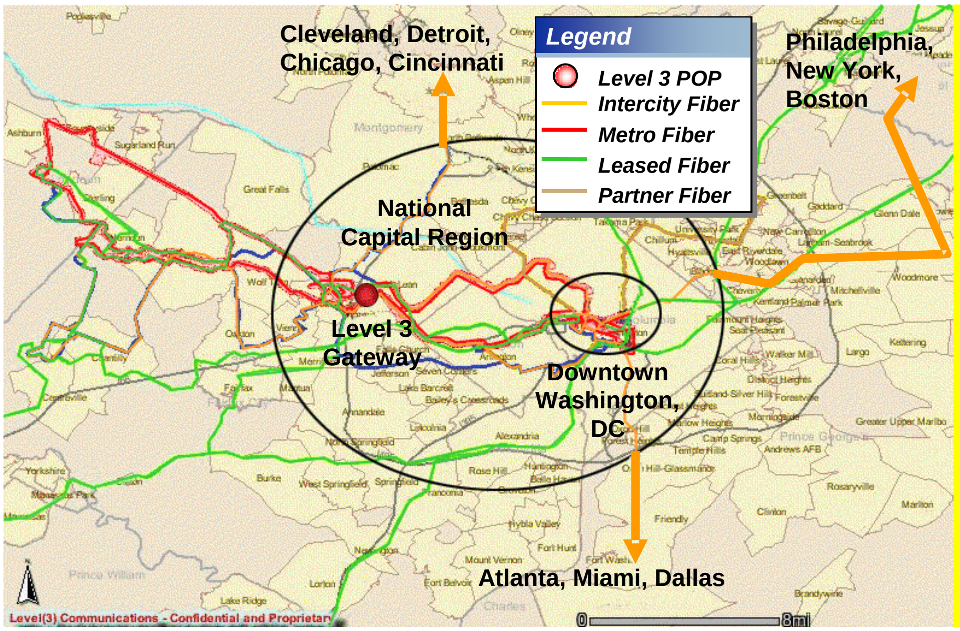


Figure A-11: The National Capital Region – multiple paths, POPs, and equipment

business district, each with 8 to 12 conduits running side by side. Each conduit was initially provisioned with a 96-fiber bundle but is capable of carrying hundreds of fibers. Today only two or three conduits are being used. Therefore the bandwidth capability for future build-outs is virtually unlimited.

There are also three POPs in the area: two synergy sites in the downtown Washington, DC area and one large gateway hub in McLean, VA. The POPs have plenty of spare capacity, routers, and switches—and are under continual reengineering to stay ahead of the growth curve. This enables Level 3 to commit to full service of all Government entities.

This extensive supply of Level 3 fiber, POPs, and equipment is located in the same area where the vast majority of Federal agencies reside. Just as the nationwide SONETS BLSR backbone protects customers from outages, the DC Metro area UPSR backbone protects city customers from outages.