Appendix C

WITS 3 Security Plan and Risks Assessment

(Req_ID 269-273, 275-278)

Level 3 Communications, LLC

Version 1

Appendix C: WITS 3 Security Plan

Report Title	Security Plan
Contractor	Level 3 Communications, LLC
Version	1.0
Date	2/10/2007

C.1 Security Management Organization and Planning

Due to the size, complexity, and geographic coverage of the Federal Government, Level 3 designed a Program Security Organization, depicted in ***Figure C-1***. Central to our security approach is the assignment of a Chief Security Officer who possesses both the technical and managerial skills to develop, contribute to, and execute a sound security plan fully compliant with the GSA WITS 3 Program [redacted]

{This Figure has been redacted.}

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted] will serve as the Chief Security Officer and is responsible for all security aspects of the WITS 3 Program. In this capacity he will oversee and ensure all activities defined in GSA WITS 3 RFP Section C.3.3.7 Security Services, are performed. He will also act as the single point-of-contact (POC) for all security management matters with the GSA WITS 3 PMO. The security program is built on and dependent upon the Level 3 Corporate Security Program and will require close coordination. This includes, but is not be limited to, such items as changes to corporate policies and procedures which impact any aspect of the security program, coordination on facility security issues, coordination on periodic testing of the Disaster Recovery Plan, and coordination on the annual budget planning process.

[redacted] developed this security plan to address the GSA's requirements and ensure that it can be executed. In addition, he is responsible for annual updates to the plan. [redacted] will represent the Security Program in the review and approval of all change requests. In addition, he will ensure the continuous improvement of the security program including the identification and deployment of new security technologies, processes, and procedures.

[redacted] is supported by and directs the security functional leads who are responsible for providing input to the overall security program and executing the security plan within their functional area. The roles and responsibilities for each functional lead are described below. The Program Chief Security Officer and the functional leads are all collocated at [redacted] will coordinate and communicate with these functional leads through informal communications such as voice and email and through formal mechanisms such as weekly status meetings and monthly GSA WITS 3 Program reviews.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.1.1 Physical Security

[redacted]

C.1.2 Personnel Security

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.1.3 Network Security

[redacted]

C.1.4 Information Assurance

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.1.5 Interfaces with Vendors, Suppliers, Partners, and Government

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.1.7 Planning

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

{This figure has been redacted}

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.2 Security Risk Management

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

{This figure has been redacted}

[redacted]

C.2.1 Risk Assessment

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

{This figure has been redacted}

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.2.2 Risk Mitigation

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

Level 3 follows a risk mitigation process based on NIST guidance as illustrated in ***Figure C-5***.

{This figure has been redacted}

C.2.5 Review and Monitor

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.3 Information Security Management

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

{This Figure has been redacted}

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.4 Information Assurance Management

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

{This Figure has been redacted}

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.5 Security Breach Response Management

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

C.5.1 Near Real Time Events/ Intrusion Detection

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.5.2 Vulnerability Remediation

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

C.5.3 Denial of Service Attacks

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.5.4 Acceptable Usage Policy

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.5.5 Escalations and Reporting

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.6 Section VI - Alarms and Audit Trails

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

C.7 Section VII - Personnel Security

[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

[redacted]

As the result of conducting the initial risk assessment, we have identified gaps and enhancements, for the Personnel Security Program to meet the unique requirements of the [redacted] in the areas of personnel classification and security training.

C.7.1 Personnel Classification

Currently, Level 3 does not have a requirement to process personnel for positions of trust.

[redacted] additional granularity must be added to identify those personnel who are in a position of trust. Procedures must be added to process those personnel using Electronic Questionnaire for Investigation Processing (e-QIP) and forwarding the forms to the [redacted] for processing. Additionally those same concepts must be applied to personnel who transfer within the program, to or from a

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

position of trust, and to employees who transfer out of the program. This will be accomplished prior to contract award.

[redacted]

- **Executive** [redacted] security incidents, business continuity, and rules of behavior.
- **General user:** This training would be targeted at all employees who participate in th[redacted] and would focus on use of the system(s), security awareness, and familiarization with the policies and procedures with emphasis on rules of behavior, access controls both physical and logical, and security incidents.

C.7.2 Specific

This training would be targeted at any employee who has a specific security role in support of the [redacted] and would focus on specific policies and procedures that correlate to that role and their designation as being in a position of trust.

It is anticipated that training will be delivered through a combination of classroom training and online courses.

C.8 Section VIII - Physical Security

[redacted] will be performed at our corporate facilities in Herndon, Virginia; Broomfield, Colorado; and Atlanta, Georgia. The [redacted] will be serviced by our robust and complete physical security program. At all these

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

locations, Level 3 has 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 and enable reviewing people and certain activities within the facilities. Certain areas of the facilities are sensitive and require another level of control. Access to these areas requires authorized personnel to have validated palm scans to gain entry. 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.

In addition to the protection of facilities, the GSA WITS 3 Program will benefit from significant physical protection of the network. This entirely optical network is more difficult to tap or access data transmitted than using signals over copper cable. Level 3 cable is terrestrial and installed within duct at a minimum burial of 48 inches. Warning tape lies above all duct banks. Fiber maintenance chambers are concrete boxes with secure 100 lb 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 the NOC as well as physically by field operations staff.

The [redacted] requires the physical protection of back-up tapes. Level 3 will provide one complete set of back-ups, both full and incremental, of all OSS data and information. This includes [redacted] software images, customer data and any other data required to fully restore all [redacted], major applications, the General Support System and all [redacted] Backup media will [redacted] housed at a vault located a safe distance from the data center. The back-up tapes enable recovery of the operating systems, production

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

data, and databases, and to restore LANs. A more detailed discussion can be found in Volume 2, Section 2.4, in response to the [redacted] RFP Section C.3.3.3

It is understood that to provide some services, Customer Premise Equipment (CPE) will be installed at facilities under Government control. The physical security of equipment at these locations is assumed to be provided by the Government and we anticipate that our technicians will be provided access, as required, for maintenance.

Prior to the installation of any Level 3 CPE, Level 3 will conduct a [redacted] to ensure that these requirements have been met; any deficiencies will be identified by the [redacted] team and forwarded to the Government for correction. [redacted]

C.9 Section IX - Procedural Security

The Level 3 total security program has been implemented with commercial best practices and is fully compliant with ISSO 177799 and SOX. Today it is documented in a number of policy and procedure documents published by various departments within the Level 3 corporate structure. [redacted], gaps between existing policies and procedures and the requirements to support FISMA and NIST SP 800-53, Annex 1 were discovered. Additionally, some tailoring of existing policies and procedures will be required to fully meet the unique requirements of the [redacted] For these reasons, Level 3 has decided to develop and implement a specific [redacted] and Procedures Manual. This document will be created from existing policies and

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

procedures, tailored to fully comply with the [redacted], and enhanced with new policies and procedures where gaps exists. This document, once completed, will contain the policies and procedures for:

- Management controls
  - Security in Life-cycle
  - Configuration Management
  - Risk Management
  - Business Continuity
  - Capital Planning
  - Incidents, Violations, and Disciplinary Action
  - Privacy Impact
  - Security Training
- Operational Controls
  - Personnel Security
  - Physical Security
  - Media controls
  - Equipment
- Technical Controls
  - Identification and Authentication
  - Access Control
  - Audit trail
  - Network Security
  - Cryptography
  - Virus Protection

We will use a combination of these procedures and the design of our OSS architecture to control access to sensitive information. Government data operational controls include the identification of employee roles to facilitate proper badging,

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

credentialing, and the appropriate background investigation. Technical controls include role-based access control, cryptography, and network security.

We will also use a combination of these controls to prevent fraudulent use of Government information or services. Level 3 will provide voice services through our Voice over IP solution. No calling cards will be issued to use this service. Technical controls are used to ensure service activation is controlled through our [redacted] access point.

C.10 Ongoing Security Refreshment

Level 3 employs an "Envision, Engineer, Operate, and Respond" lifecycle that provides a continuous capability to ensure processes and systems are optimized to their fullest extent. An engineering and architecture group is maintained that is responsible for the research, development and integration of security mitigations solutions within the network architecture. This will give the [redacted] ongoing refreshments. In many cases, this involves an analysis of off-the-shelf security products, to identify "best-of-breed" solutions. The group focuses much of its effort on analyzing best practice models to identify enhancements or new capabilities to the security architecture.

Level 3 regularly conducts security review meetings with industry peers and law enforcement agencies to identify the latest trends and movements within the security arena. This ensures current, proper practices are in place within the network.

The GSA WITS 3 Program will benefit from our well maintained Security Engineering lab which is used to provide evaluation and assessment to the Security Engineering Department. This facility plays a critical function in keeping the Security Engineering Department up-to-date on security issues that may have an operational impact on the network. The Security Lab regularly reviews commercial security products and performs assessments on the network, systems, and applications, and tests and verifies the application code used within the infrastructure.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

As a charter member of the Internet Services Provider (ISP) Security Consortium, Level 3 has pledged to work with ISPs on specific detection, prevention, and tracing options that can be deployed industry-wide. The [redacted] needs a provider dedicated to researching new attacks, attack methodologies, vulnerabilities, and security compensators. Level 3 will provide the above as well as participate in the Telecommunication Information Sharing Analysis Center (ISAC). The Security Engineering Department develops and maintains a security infrastructure for the Level 3 production systems, OSS and service component software. This team proactively collects and analyzes new security threat information in a variety of ways, including the following:

- Security mailing lists (bugtraq, ISN, Firewalls, plus 54 others)
- Security advisory lists (CERT, CIAC, AUSCERT, plus 17 others)
- Industry Security Advisory Groups (ISPSEC, FINNA, CSI, plus five others)
- Federal Security Advisory Groups (NSTAC, NSIE, IRSCIS, plus three others)
- "Security Underground" sources
- Manual research operations for "deep-dive" analysis of security exposures
- Patch Management

We will automatically collect and analyze security-related data from multiple sources to identify new threats, review security product news, and analyze security patches. These data are collected from more than 2,200 sources on a daily basis, including mailing lists, new groups, Web sites, ftp sites, and chat rooms. All threat data are collected and analyzed for potential exposure in a network-engineering laboratory. Once compensators have been identified, they are deployed in the field.

C.11 Non-Domestic Services Security Management

Not applicable. Level 3 is not bidding non-domestic services.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.12 Fraud Detection and Prevention

The Level 3 Fraud Prevention group monitors, responds to and investigates fraudulent activities associated with the misuse of network services, systems, and information. The Level 3 Information Security Officer manages and oversees fraud prevention activities and is a member of the Network Operations team.

A critical component to voice fraud is the underlying network and systems. Several layers of network and host security, as well as system and application access controls protect Level 3 systems and information. These network and system controls are used to protect both Level 3 and customer information contained on Level 3 systems.

For VOIPTS off-net calls handled by Level 3 on the [redacted], there are several fraud abuse and detection capabilities available. Level 3 utilizes an industry-leading fraud system to monitor over 35 million voice call records in near real-time per day. Alarm thresholds consist of rules, watch-points, and a profiling engine. In addition, the calling card platform's usage is monitored by a separate, real-time application. Fraud detection activities, such as message and calling pattern analysis, are performed prior to the detail billing cycle, and all records and audit trails are used for fraud analysis after the billing cycle completes.

The Level 3 Fraud Center is staffed 24x7 to monitor and detect potential fraudulent voice traffic. Detailed analysis is performed when a potential fraudulent case is identified by the monitoring system. Investigating suspected fraud on a voice service is simply a process of dissecting a call and analyzing its various pieces. Starting with the call(s) that initially triggered an alarm, a fraud analyst first looks at where the call originated and terminated. International terminations are much more likely to result in fraud than domestic calls, so many domestic calls can be quickly ruled out as legitimate unless other factors are present.

Next an analyst looks at the type of call. Certain types of calls such as third party, collect and calling card are more susceptible to fraud than are long distance calls.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

We also look at Automatic Number Identification (ANI) information digits to determine if the call(s) originated from a pay station, cellular phone or prison phone. Calls originating from one of these sources are more likely to be fraudulent than calls originating from regular Plain Old Telephone Service (POTS) numbers. At some point, we also look at the call history for the alarming line of service.

The customer is notified of fraudulent activities based on contractual requirements. When customer notification takes place, relevant alerts and pertinent call history are provided to the customer.

Level 3 takes a proactive approach in developing methods to prevent, detect, and report fraudulent use of all services. The following text describes the Level 3 approach for modernizing with the latest fraud prevention and detection trends, methods, and technologies and for improving fraud detection prevention capabilities throughout the life of the contract. The Security Engineering team constantly researches and investigates the latest technologies, processes and procedures in fraud prevention, detection and analysis. This team also interacts with customers to integrate changes into existing processes and systems. New capabilities will be merged into the [redacted] over the life of the contract that will [redacted] on our commercial, private-sector services and systems. Further details on our security refreshment program can be found in 2.3.1, Section X – Ongoing Security Refreshment.

C.13 Improved Security-Related Processes and Technologies

Level 3 embraces a culture of constant technology improvement and process refinement. A recent example was the deployment of the rogue detection system and corresponding procedures. Specifically, in 2004 Level 3 recognized the need to augment its security infrastructure with a capability to quickly and proactively detect unauthorized and misconfigured systems and wireless devices that connect to its

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

enterprise network. Early detection of unauthorized or infected systems is essential to protecting the network, especially if such systems have access to other trusted resources that corporate firewalls and security systems could not protect.

To mitigate this risk, Level 3 internally developed a rogue detection system that can detect and interrogate system or wireless devices attempting to connect to our internal network. The rogue detection system in turn limits access to authorized Level 3 devices based on device type and Media Access Control (MAC) address. In addition the device must have the complete array of security and anti-virus tools installed. Any device failing to meet these security policy criteria is automatically removed from the network, and placed onto the rogue network, at the layer 2 VLAN level, which has no access to the rest of the internal network. We also use the rogue VLAN to quarantine any virus infected system to prevent the spread of viruses as well as allow for the security team to remotely clean and repair the system, upon detection by our Intrusion Detection Systems.

We built a robust set of processes around the rogue detection system to ensure it is appropriately used and is sensitive to the productivity needs of business. The procedures allow for timely troubleshooting of rogue systems, installation of security tools, registration of new device types, and temporary exception requests. Many of these processes have since been automated based on the detailed procedures and our culture of continuous improvement.

In the commercial services portion of Level 3's infrastructure, constant improvements are being developed and implemented. Since the commercial services infrastructure uses an ISO 17799 framework any improvements and procedures will follow that paradigm. Many of the improvements are based on new products, policies, and procedures along with custom, in-house developed technologies that check and enforce host configurations and detect rogue device attachments to protected segments.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

The Level 3 security lifecycle process of “Envision, Engineer, Operate and Respond” includes a rolling 12 month security roadmap that works to ensure all tactical and strategic security initiatives are brainstormed by all relevant business security stakeholders. This roadmap serves as the process by which new technologies are planned for within the network, and then tactically achieved.

Those technologies, processes and procedures inherent in the commercial Level 3 OSS that are, or can be made, FIPS compliant will be migrated or duplicated in the [redacted] that Level 3 is building. While the FIPS do not specify any technologies, processes or procedures that are “new” in the industry, there are some FIPS required technologies that will be “new” to Level 3. FIPS 201 compliant SmartCard access to the facilities and technical infrastructure in the [redacted] is an example. There will also be the implementation of certificate based authentication mechanisms for the Government facing portal so that authorized agency staff can access the agency support portal functions as required by FIPS 201. The public RSA key from the users SmartCards will be used as the only access mechanism to the non-public areas of the web portals, support applications, monitoring systems, etc.

As FIPS 199 Impact Level Low compliant technologies, processes and procedures become available they will be incorporated into the [redacted]

C.14 Risk Assessment

C.14.1 Introduction

Purpose: The purpose of this initial risk assessment is to identify security requirements and determine which are not currently being met during the initiation phase of the system development life cycle. Risks identified during this assessment will be addressed during the development phase to ensure that appropriate controls will be in place prior to implementation.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

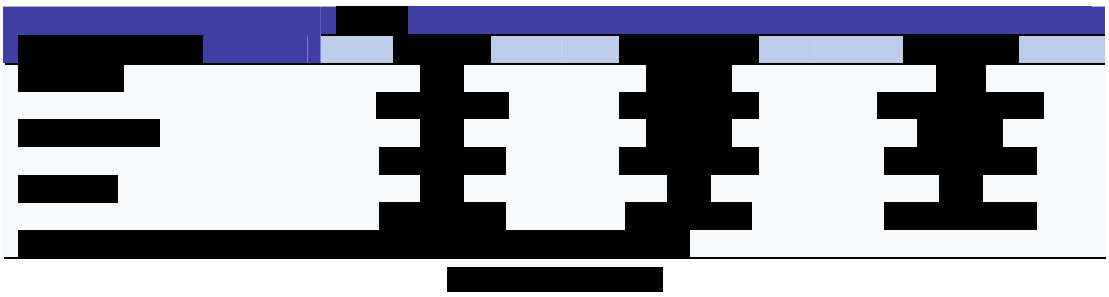
Scope: This risk assessment addresses risks to [redacted] including:

- Order Entry Service Activation
- Billing
- Trouble Ticket/Network Management
- Metrics

[redacted]

C.14.2 Risk Assessment Approach

This initial risk assessment was conducted during the Initiation Phase of the Synchronous Data Link Communication (SDLC) by an independent contractor who followed the methodology identified in NIST SP 800-30, *Risk Management Guide for Information Technology Systems.* Requirements were developed from guidelines contained in Annex 1 to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.* Techniques used to gather information included document reviews and interviews with Level 3 management, technical and security personnel. The assessment used a 3x3 risk scale as described in [redacted]



The assessment focused on the Level 3 Security Program and practices that provide the framework for implementing specific system level security controls. The final risk assessment will provide a more thorough review of specific management, operational and technical controls as implemented.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

Level 3 has divided the [redacted] into six separate systems, or system areas, for the purpose of the Security Plan and Security Program Management. The six system areas are:

- Order Entry and Order Activation
- Network Management and Service Management
- Partner System(s)
- Client Portal
- Billing
- Reporting

Each system boundary includes servers comprised of various hardware platforms, operating systems and applications as well as their own switches and routers and other infrastructure resources. Level 3 hosted systems are segregated from our commercial OSS and infrastructure by firewalls, intrusion detection and preventions systems, and anti-virus technologies dedicated to the [redacted] and managed under the Level 3 Federal Security Management Program.

WITS 3 data is retained within their respective system boundaries or with the overall WITS 3 OSS cumulative system boundary until archived or downloaded by the client agency. Offsite archives are encrypted with FIPS 140-2 compliant algorithms before leaving Level 3 premises.

Connectivity between system boundaries, such as between sub-contractor [redacted] is accomplished through dedicated links using IPSec with encryption modules compliant with FIPS 140-2.

C.14.3 Threat Statement

[redacted] provides a list of vulnerabilities identified during this assessment and identifies the potential threat sources and associated threat actions applicable to [redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

Vulnerability	Threat Source	Threat Action
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

Vulnerability	Threat Source	Threat Action
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

C.14.4 Risk Assessment Results

This section contains the findings of this risk assessment and includes the following:

- A summary of vulnerabilities identified during this assessment
- The likelihood that threat sources identified in Table 2.3-4 could exploit those vulnerabilities
- The magnitude of impact if vulnerabilities were exploited
- The assessed level of risk based on the risk scale matrix provided in Table 2.3-3
- A strategy for mitigating each vulnerability

Definitions for likelihood and impact magnitude are provided in Tables [redacted] and [redacted], respectively, and risk descriptions and required actions are provided in Table [redacted] Results of the assessment are provided in Table [redacted].

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of
data contained on this sheet is subject to the restrictions on the title page of this proposal.

Vulnerability	Existing Mitigating Controls	Likelihood	Impact	Severity	Recommended Mitigation Strategy
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

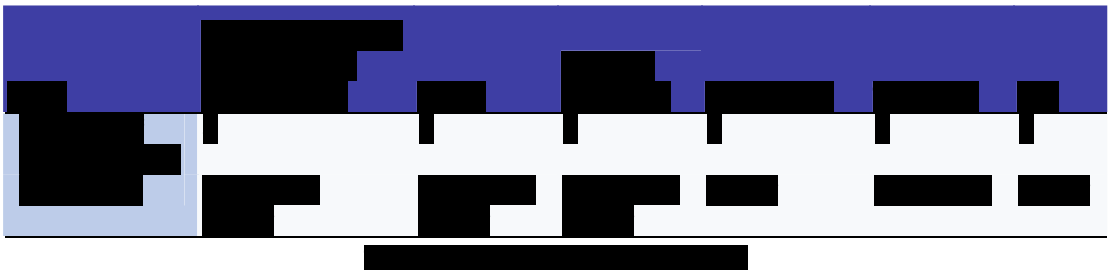
Vulnerability	Existing Mitigating Controls	Likelihood	Impact	Severity	Recommended Mitigation Strategy
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

C.14.5 Summary

This initial risk assessment was conducted on a system in the initiation phase of the life cycle. It was conducted by reviewing documents and interviewing key personnel. There was no testing conducted to verify that controls were actually implemented as designed. The objective of this assessment was to identify gaps between requirements and existing controls so that they can be addressed during the development phase to ensure that appropriate controls will be in place prior to implementation. A final risk assessment of this system and its major components will be conducted as part of the certification and accreditation process before this system is fully implemented.

Twelve vulnerability areas were identified where security controls did not meet FISMA requirements or NIST guidance. Risk levels assigned to these vulnerabilities were medium and low. There were no high risks identified. A summary of vulnerabilities and associated risk levels is provided in [redacted]



© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.