Appendix E

Level 3 Fraud Prevention Procedures

1.1 Appendix E: Fraud Prevention Procedures

One of the most critical security operations on every program to assure the quality of services offered. Level 3 has built fraud management capabilities into our network monitoring and management systems to ensure this on all of our programs. These capabilities include user access to systems through authentication mechanisms and passwords and use of authorization codes to control a customer's exposure to potential fraud. Within this section, Level 3 provides our internal policies for prevention, detection and reporting of fraudulent use of services. These procedures will be maintained and updated on a regular basis throughout the life of the WITS 3 contract.

1.2 E.1 Policy for Prevention, Detection, and Recording of Fraudulent Use of Services

Level 3's Fraud Prevention Group monitors, responds to, and invetigates 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.

1.2.1 E.1.1 Proactive Fraud Prevention

Level 3 continually conducts security audits of our systems to determine what risk of potential fraud exists. These security audits include assessments of physical security, systems security, network security, and analysis of anti-fraud measures. Based upon this audit, Level 3 prepares a Security Audit Report that discusses the strengths and weaknesses of the security and anti-fraud mechanisms, and makes specific recommendations as to areas requiring improvement.

As part of Level 3's proactive approach to fraud prevention, our 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 WITS 3 systems over the life of the contract that will match or exceed those on our commercial, previate-sector services and systems.

1.2.2 E.1.2 Fraud Monitoring and Detection

The Level 3 Fraud Center [redacted]

[redacted]

1.2.3 E.1.3 Fraud Reporting

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]