Appendix 12
Risk Assessment Plan

DRAFT

December 13, 2006

Revision XX

Qwest Government Services, Inc.
4250 North Fairfax Drive
Arlington, VA 22203

REVISION HISTORY

Revision Number	Revision Date	Revision Description	Revised by

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

The Qwest risk management and information security mission is to protect the integrity, confidentiality, and availability of information assets and supporting resources of the network.

The Qwest Team will provide all required security controls, network surveillance, network element security management, and managed security solutions, ensuring Qwest meets the Government's security mandates as described within the Networx Universal RFP.

The Qwest Team will provide to the Agencies, information security expertise, risk analysis, evaluations, and guidance to ensure Qwest complies with Government policies, standards, and requirements. The Qwest Team focus will be on:

[redacted]

1.1 CONTENT AND PURPOSE (C.3.3.2.4.2.1.4)

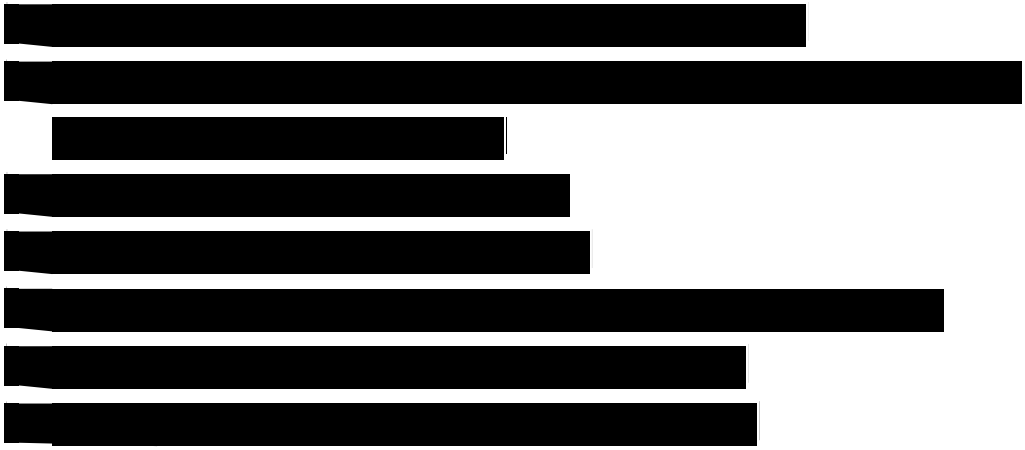
The purpose of a risk analysis is to identify to the GSA Networx PMO, security vulnerabilities and associated risks that may impact the security posture of Qwest provided Networx services. The Qwest Risk Assessment Plan outlines a risk analysis and subsequent report of the Networx related services, the Networx service infrastructure and OSS. Qwest is not proposing an Agency specific Risk Assessment in addition to a Risk Assessment of our Networx service infrastructure and OSS.

The risk analysis process focuses on identifying vulnerabilities within the services infrastructure (e.g., operating system or network element flaws, architectural concerns), as well as enumerating the threats applicable to specific Networx services. Together, this threat model and set of known vulnerabilities provide a clear picture of risk and the specific actions required to manage them appropriately. Qwest will also conduct security control assessments of our Networx domestic/non-domestic sub-contractors/partners/suppliers. Working with the CPO Subcontract Manager, the Qwest Networx Security Manager is responsible to ensure the integration of flow down contract language to address process-based security control assessment. This approach will ensure that physical security controls are in place with Qwest's domestic/non-domestic subcontractors, partners, and suppliers who have access to Government information. In addition, Qwest will maintain situational awareness on all subcontractors, partners and suppliers that may handle Government information through the daily monitoring of security related activities, including the re-evaluation and recommendation of security controls. The results will be reported to the Qwest Networx Security Manager who in turn will re-evaluate the risk and impact and effect any necessary control changes. Qwest will keep a log of any of the control changes that will be included in the yearly risk assessment.

Through our enterprise Risk Management organization, Qwest has existing processes and the proven expertise to drive this kind of holistic recognition and management of risk. In addition to the services and infrastructure provided by Qwest, such an analysis must also consider the state of information security practice and infrastructure risk present at specific Agency customer locations. Because this risk analysis requires a clear scoping of specific services provided, along with detailed information sharing from the customer, Qwest will prepare a risk assessment report to

communicate actions taken to maintain the Government's security environment at an acceptable level of risk for both Qwest and the Government. This will begin within 30 days of the Notice to Proceed, followed by periodic updates according to the customer's requirements.

Security risks evolve over time as technologies change, vulnerabilities are discovered, and the threat climate evolves. Through our partnership with the GSA Networx PMO and the Agencies, Qwest will ensure risks are identified and managed in a timely manner according to the customer's requirements. In future Risk Assessment reports for the Government, the following areas will be discussed:



1.2 APPLICABILITY

Risk analysis activities, processes, and procedures identified within the risk assessment report will apply to the Government's data, information systems, telecommunications infrastructure, products, and services as identified within the Networx Universal RFP.

Beginning within 30 calendar days of the Notice to Proceed, Qwest will provide the Networx PMO a revised Security Plan, including an updated risk assessment report, followed by periodic updates as required.

The following sections of this initial risk assessment attachment covers the applicable laws and a general overview of mitigation strategies used by Qwest to mitigate risks, along with recommended actions for Agencies to take where the risk to be addressed has components that lie outside the boundaries of the services provided.

1.3 APPLICABLE LAWS, REGULATIONS AND POLICIES AFFECTING NETWORX NETWORK INFRASTRUCTURE

The laws, regulations, and policies shown in ***Figure A12-1*** will be used to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.

Figure A12-1. Laws, Regulations and Policies Affecting Networx Network Infrastructure

Law, Regulations and Policies	Purpose
National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2	Security Requirements for Cryptographic Modules
NIST FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems (Pre-Publication Final)
NIST Special Publications (SP) 800-12	An Introduction to Computer Security: The NIST Handbook
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-18	Guide for Developing Security Plans for Information Technology Systems
NIST SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
NIST SP 800-26	Security Self-Assessment Guide for Information Technology Systems
NIST SP 800-30	Risk Management Guide for Information Technology Systems
NIST SP 800-31	Intrusion Detection Systems (IDS)
NIST SP 800-34	Contingency Planning for Information Technology Systems

Law, Regulations and Policies	Purpose
NIST SP 800-35	Guide to Information Technology Security Services
NIST SP 800-36	Guide to Selecting Information Technology Security Products
NIST SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
NIST SP 800-40	Procedures for Handling Security Patches
NIST SP 800-41	Guidelines on Firewalls and Firewall Policy
NIST SP 800-42	Guideline on Network Security Testing
NIST SP 800-45	Guidelines on Electronic Mail Security
NIST SP 800-46	Security for Telecommuting and Broadband Communications
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems
NIST SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program
NIST SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
NIST SP 800-53	Draft Recommended Security Controls for Federal Information Systems
NIST SP 800-55	Security Metrics Guide for Information Technology Systems
NIST SP 800-59	Guideline for Identifying an Information System as a National Security System
NIST SP 800-61	Draft Computer Security Incident Handling Guide
NIST SP 800-64	Security Considerations in the Information System Development Life Cycle
NIACAP (NSTISSI 1000)	National Information Assurance Certification and Accreditation Process
DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (DoD 5200-40)	DoD Information Technology Security Certification and Accreditation Process

In addition, Qwest adheres to the following standards and acts:

- E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA))
- T1.276-2003 American National Standard for Telecommunications — Operations, Administration, Maintenance, and Provisioning Security

Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

- All commercially available standards for any applicable underlying access and transport services
- All new versions, amendments, and modifications made to the above listed documents and standards, when applicable and commercially available
- Public Law 100-235, *"Computer Security Act of 1987,"* January 8, 1988
- Bellcore Gr-815, Network Element and Network System Security
- Homeland Security Presidential Directive / HSPD-5, February 28, 2003
- Homeland Security Act of 2002 Public Law 107 296
- Qwest Communications Physical Security Construction Standards
- Qwest Policy [redacted] and all other applicable Qwest policies and standards designed to address security management

1.4 TECHNICAL APPROACH TO SECURITY ASSESSMENT

[redacted]

[redacted]

[redacted]

1.5 SECURITY RISK MANAGEMENT

Qwest's security risk analysis processes address infrastructure components, such as routers, Ethernet switches, firewalls, and servers, as well as the processes used to maintain them, along with the environment used to deliver specific security services to Agencies. Networx OSS and Government information stored on or made available by the OSS will be included in the security risk analysis process.

[redacted]

Qwest will conduct security risk analysis, reviews, or evaluations of Networx services throughout the life of the contract annually as required in the Networx contract. The objective of these reviews is to provide verification

that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for Networx services.

By using this comprehensive process, we ensure the security of Networx services does not degrade over time as the technology and the systems evolve, or people and procedures change. Periodic review provides assurance that management, operations, personnel and technical controls are functioning effectively and providing adequate levels of protection.

1.6 REPORTING POTENTIAL IMPACTS

Qwest will use FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, which contains the potential impact categorization definitions, (Low, Medium, or High). Qwest will apply these standards to all Networx security analysis activities and risk assessment reports. The application of these definitions must take place within the context of each Agency participating in the Networx contract.

1.7 SECURITY RISK ANALYSIS

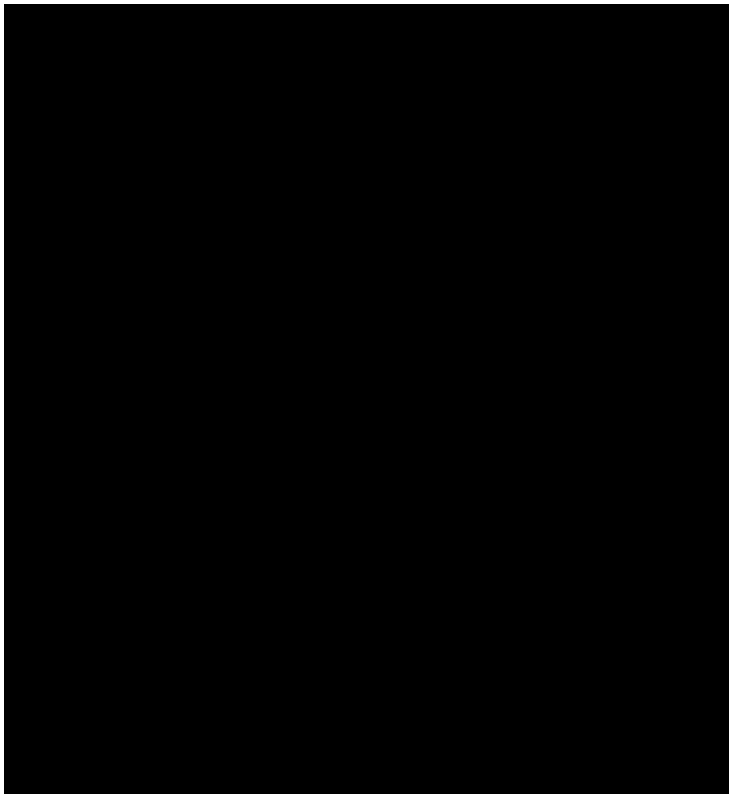
Qwest security risk analysis responsibilities are assigned to specific technology operational groups within Qwest. [redacted]

[redacted] As stated in Section C.3.3.2.2.2, security risk analysis, Qwest will conduct annual security risk analysis, reviews, and/or evaluations of Networx services throughout the life of the contract. The objective of these reviews is to provide verification that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for Networx services.

All security risk analysis activities will adhere, at a minimum, to the following:

- NIST SP 800-30, July 2002
- NIST SP 800-53, February 2005
- Federal Information Processing Standards (FIPS) Publication 199, February 2004

The following flowchart [redacted] identifies the Qwest Team mitigation methodology used throughout the Networx Security Risk Analysis process.



1.8 INFORMATION SECURITY MANAGEMENT

Section 4.0 in the Security Plan details Information Security Management controls and processes. [redacted] summarizes the scope of the Qwest infrastructure security management architecture.

[redacted]

Qwest's Network Security System and capabilities provides Networx customers with a high level of confidence in network information security and reliability [redacted]

[redacted]