

Qwest Security Plan

For RFP WTT-98-PW-N-0001

July 25, 2003

Version 1.0



Prepared for:

General Services Administration

Prepared By:

Gary Morgan

Qwest Communications Corporation

555 17th St

Denver CO.

This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed -in whole or in part- for any purpose other than to evaluate this service/product description. This restriction does not limit the Government's right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction are contained on all sheets of this proposal.

Foreword

The *Security Plan* is a single source for all information pertaining to Request for Proposal (RFP) for Qwest services and provides a government schedule as it pertains to security resources that are required within the scope of this document. As such, it either contains or references the information necessary for the contracting office to make a decision regarding Statement of Work or contracting proposal.

The *Security Plan* contains **SENSITIVE AND RESTRICTED** information that pertains to Qwest Corporate system functions, descriptions, and vulnerabilities. To ensure that this document is released to authorized personnel, it is marked "QWEST PROPRIETARY". All Qwest Corporate documentation that is referenced in this Security Plan will be maintained at the Qwest Program Office. This documentation will only be released to those individuals who have a valid Need-to-Know. All individuals who require access to this information will be required to sign a Qwest Non-Disclosure Agreement prior to review.

1.1 REQUEST FOR PROPOSAL (RFP) REQUIREMENTS

The requirements below are instituted IAW WITS2001 CROSSOVER PROPOSAL REQUIREMENTS RFP WTT-98-PW-N-0001 dated January 11, 2002 and RFP WTT-98-PW-N-0001 Amendment 0010 dated September 28, 1999. AND subsequent amendments, **IAW Table A-1. STIPULATED BASIC REQUIREMENTS COMPLIANCE CHECKLIST items 156-158 and 245 to 250 and Table A-2. REQUIRED NARRATIVE RESPONSES (ELIGIBILITY PROPOSAL) 2,6,7, and 8** the Qwest Government Security Plan.

1.1.1 Proposal (RFP) Requirements

[Reference C.6.6 - Protection of Classified and Sensitive Information](#)

The contractor shall provide for the protection of Sensitive but Unclassified (SBU) communications commensurate with NCSC-11 and NTISSP No. 1. The contractor shall engineer, acquire, provision, install, operate, administer, and maintain the protection equipment at the facility locations where the contractor has proposed to install applicable equipment. Essentially, any unclassified information related to the national defense or foreign relations of the United States, to include bits and pieces that in the aggregate would be even more revealing, that could be useful to an adversary, should be considered UBS information. The contractor shall follow commercial practice to protect its sensitive systems. These sensitive systems include:

1. Databases for classified information
2. Critical subscribers' locations, identifications, authorization codes, and call records
3. Customer profiles
4. Computer systems that control or can control the network or services

The contractor will be provided access to classified and sensitive materials required for service restoration planning, management, and operations. That information will be in various forms, including hard copy and electronic media. The classification of the material will be identified and must be protected by the contractor in accordance with applicable industrial security regulations (*National Industrial Security Program Operating Manual [NISPOM] for Safeguarding Classified Information*). The level of classification will be up to and including Top Secret. The contractor shall protect SBU with the same level of protection required of "For Official Use Only" (FOUO) information as defined by industrial security regulations.

Reference C.3.3.6 - Physical Security and Work Area Management

The contractor shall follow security procedures established by the Government in conjunction with building management to prevent unauthorized access to a building's telecommunications facilities (e.g., telephone closets). [REDACTED]

Reference C.3.3.7 - Security Services

Telecommunications services provided under this contract will carry non-sensitive programmatic and administrative traffic, SBU traffic, and higher levels of traffic that have been encrypted by users. Therefore, appropriate security services are required. The contractor shall provide security services that are compatible with existing security devices and systems used by the Government. The contractor shall ensure that these services protect all facilities and services, portions of the contractor's network used to provide WITS2001 services, information, and information processing resources provided under this contract against threats, attacks, or failures of systems.

The contractor shall provide security within the infrastructure of the WITS2001 network against threats [REDACTED] consistent with commercial practice, which shall ensure availability of service, confidentiality, and data integrity of the WITS2001 transmission and switching systems, the support systems, and the databases being maintained by the contractor in support of WITS2001 services. Only authorized Government personnel (as determined by the GSA ACO) shall have access to those portions of the infrastructure of the WITS2001 network that are determined by the contractor to be off limits.

The contractor shall monitor potential security problems on an ongoing basis and alert WITS2001 customers (e.g., by telephone or e-mail) of threatening situations. The contractor shall give customers the option of pre-authorizing the contractor to disable access to the Internet during a security event that the contractor deems to be serious.

The contractor's Security Plan with outlines the risks and the risk avoidance methodology and management that are to be implemented upon contract award. The Security Plan shall be updated semiannually and shall address all aspects of security, identify major risks, and discuss how best to mitigate these risks. The Security Plan must be approved by the Government prior to acceptance of support systems or any service.

1.1.2 Requirements RFP Compliance Checklist

The contractor shall provide for the protection of SBU communications commensurate with NCSC-11 and NTISSP No. 1. The contractor shall engineer, acquire, provision, install, operate, administer, and maintain the protection equipment at the facility locations where the contractor has proposed to install applicable equipment. [REDACTED]

The contractor shall protect SBU information with the same level of protection required of "For Official Use Only" (FOUO) information as defined by industrial security regulations. [REDACTED]

The contractor shall follow commercial practice to protect its sensitive systems. These sensitive systems include: [REDACTED]

The contractor shall follow commercial practice to protect its sensitive systems. These sensitive systems include: [REDACTED]

The contractor shall follow commercial practice to protect its sensitive systems. These sensitive systems include: [REDACTED]

The contractor shall follow commercial practice to protect its sensitive systems. These sensitive systems include: [REDACTED]

1.1.3 Required Narrative Responses (Eligibility Proposal)

The contractor shall provide security services that are compatible with existing security devices and systems used by the Government. The contractor shall ensure that these services protect all portions of the contractor's network used to provide WITS Program services, information, and information processing resources provided under this contract against threats, attacks, or failures of systems.

The contractor shall provide security within the infrastructure of the WITS Program network against threats [REDACTED] consistent with commercial practice, which shall ensure availability of service, confidentiality, and data integrity of WITS Program transmission and switching systems, the support systems, and the databases being maintained by the contractor to support WITS Program services. Only authorized Government personnel (as determined by the GSA ACO) shall have access to those portions of the infrastructure of the WITS Program network that are determined by the contractor to be off limits.

The contractor shall monitor potential security problems on an ongoing basis and alert WITS Program customers (e.g., by telephone or e-mail) of threatening situations. The contractor shall give customers the option of pre-authorizing the contractor to disable access to the Internet during a security event that the contractor deems to be serious.

1.2 SECURITY PLAN REQUIREMENTS

Qwest, through its Information Systems Administrators (SA), will plan, direct, coordinate, control and implement Qwest Security Policies stipulated in the Qwest Security Plan. Qwest Information Systems will be developed on Controlled Access protection model (C2) using the best industry practices. Information Systems Security Managers will implement Qwest Network Security Policies as promulgated in the Qwest Security Plan herein. The Information SA will develop individual/group access control list (ACLs) to allow users specific control of an asset or sharing of an asset by named individuals, or defined groups of individuals, or by both, and will provide controls to limit access rights based on level of clearance and the need to know.

Purpose

The purpose of this security plan is to provide framework for implementation of security requirements IAW with the Rainbow Series as required by the RFP herein. Qwest security policies (reference governing security requisites) were derived from the Rainbow Series/NIST 800-18 “criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, responsibilities promulgated by OMB 130 and Qwest Best Practices

Scope

The trusted computer system Security criteria defined in this document apply primarily to trusted commercially automatic data processing (ADP) systems as applied in the development, implementation and testing of the Qwest Network. The implementation of the security criteria is applicable in the development, implementation, test/evaluation of security requirement for systems acquisition. The trusted computer system Security criteria defined in this document include two distinct sets of requirements: 1) specific security feature requirements, and 2) assurance requirements. The specific feature requirements are information processing systems such as general-purpose operating systems where applications programs are employed such as [REDACTED]. The assurances are to systems that employ computing environments from controllers and a full range multilevel secure resource sharing systems.

Fundamental Computer Security Requirements

In order to implement a security framework, we must define and identify the fundamental objective of Computer Security. A security policy will be defined as policies or operating procedures used to secure computer system which will control access to information where authorized users or processes will have access to read, write, create, or delete data. From this conceptual framework we derived specific requirements to meet the security policy objectives. From this framework we identified requirements associated with the creation of a trusted computer system.

1.4 DATA SECURITY REQUIREMENTS

Qwest security policies for WITS (reference governing security requisites) were derived from Qwest Best Industry practices , NIST , Rainbow Series “Security Requirements ,” IAW OMB Directive 130 issued under the authority in accordance with public law “Its purpose is to provide Mangers/Supervisors direction and guidance for implementation of technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and protection of critical infrastructure as promulgated by Congressional Mandates and Executive Order.

Scope

The trusted computer system Security criteria defined in this document apply primarily to trusted commercially automatic data processing (ADP) systems as applied in the development, implementation and testing of the Qwest Network. The implementation of the security criteria is applicable in the development, implementation test/evaluation of security requirement for systems acquisition. The trusted computer system Security criteria defined in this document include two distinct sets of requirements: 1) -- [REDACTED] and 2) [REDACTED]. The specific feature requirements are information processing systems such as general-purpose operating systems where applications programs are employed such as communications processors, process control computers, and embedded systems. The assurances are to systems that employ computing environments from controllers and a full range multilevel secure resource sharing systems.

Data Security Requirements

Security Policy - Security policy must be defined and enforced by the system to control access to a system or component within the domain and to protect the system from access by an unauthorized entity. Domain elements must translate security policy for handling SBU into discretionary security access controls as required to ensure that only selected users or groups obtain access to data based on the security level and the need-to-know. [REDACTED]

Security Policy/ Discretionary Access Controls

The Qwest Network I operates in multiple domains the access controls deployed will be capable of including or excluding access to the granularity of a single user or a group of users. Reference Figure 1-1:

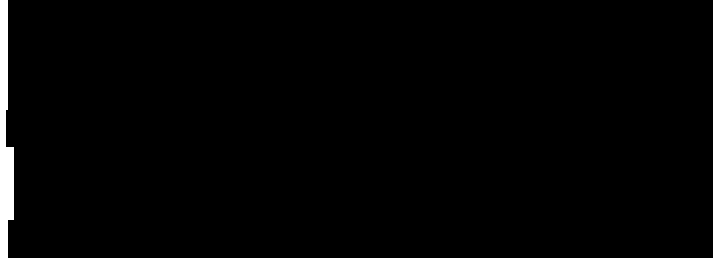


Figure 1-1

The Qwest Network will process or handle classified and/or SBU information and will require at least controlled access protection class C2 security, based on the risk assessment procedure described in DoD 5200.28.

Systems representative of classes are defined and identified C thru A. These controls are hierarchical in nature and are progressively rigorous starting with the least protection C to the most protection A.

- C1 - Discretionary Security Protection
- C2 - Controlled Access Protection
- B1 - Labeled Security Protection
- B2 - Structured Protection
- B3 - Security Domains
- A is the highest security division

Identification - Individual that has access to the domain must be identified. Access must be mediated by classes of information they are authorized by the use and implementation of ACLs. The identification/authorization must be securely maintained by the computer system that performs security-relevant action in the system. ACLs will be developed for -domain based on the users authorization and the need to know.

Accountability -The domain will have the capacity to protect from modification, unauthorized access or destruction of an audit trail to the objects it protects. The DOMAIN will allow access only to personnel authorized to audit information will protect audit information. The DOMAIN will be able to record events such as of identification and authentication, file open, program initiation, deletion of objects, actions taken by users i.e. computer operators and system administrators, etc, and all significant system events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request, terminal ID will be included in the audit record. DOMAIN administrator will have the capacity to audit the actions users based on individual identity.

Security Policy – Qwest operates [REDACTED]. All personnel that have access to the domain will have proper authorization and the need to know. Discretionary access controls are required to

QWEST PROPRIETARY

ensure that only selected users or groups of users may obtain access to data based clearance on a need-to-know).

Assurance - The computer systems must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements ACCOUNTABILITY SECURITY POLICY listed above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.

DISCRETIONARY ACCESS CONTROLS C2

Security Policy Implementation

The administrative domain processes classified and/or sensitive unclassified information that require at least controlled access protection class IAW C2 security based on the risk assessment procedure described in Rainbow Series, Qwest Best practices, and NIST Standards.

Qwest Information's Systems will be developed on [REDACTED]

Systems Security Administrators [REDACTED]

Systems Security Administrators [REDACTED]

Access controls will have the capability of including or excluding access by a single user.

Authorized users (Network Administrator) may only assign access.

Limited access rights will be based on level of clearance and the need to know.

Access Control Lists (ACLs) will be kept current and will be swept IAW Qwest Standards when required due to employment termination or reassignment.

Object Reuse

The system must have the capacity to avoid the reuse of deleted Objects.

ACCOUNTABILITY

Identification and Authentication

The DOMAIN will identify the user before beginning to perform any other action.

QWEST PROPRIETARY

Use or disclosure of information contained on this page is subject to the restrictions on the title page.

QWEST PROPRIETARY

The DOMAIN will have identification/authentication procedures for users such as Username/Password.

The resource must protect authentication information from access by unauthorized users.

The DOMAIN will have the capability to identify each individual system user.

Audit

The DOMAIN will have the capacity to protect from modification, unauthorized access or destruction of an audit trail to the objects it protects.

Audit information will be protected by the DOMAIN to allow access only to personnel authorized the audit information.

The DOMAIN will be able to record events

For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request, terminal ID will be included in the audit record.

The DOMAIN administrator will have the capacity to audit the actions users based on individual identity.

Operational Assurance

System Architecture

Security Administrator will create and maintain the domain and protect it from tampering, unauthorized use, programming; logical, physical, or structural modification.

Resources controlled by the domain may be a defined subset of the subjects and objects in the DOMAIN. The domain shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

System Integrity

The DOMAIN will employ hardware/ software features to periodically validate the correct operation of the on-site hardware and firmware elements of the DOMAIN.

Conduct Random audits of systems Hardware/ software features

Conduct system audits to ensure the latest hot fixes from the vendors are deployed and working.

Ensure the latest anti-viral scans are loaded on all systems with in your domain.

Ensure you are on distribution for all security bulletins, patches, anti-viral scans, issued by vendors

QWEST PROPRIETARY

Use or disclosure of information contained on this page is subject to the restrictions on the title page.

Regularly install updated anti-virus signature files from your anti-virus vendor.

Life-Cycle Assurance

Security Testing

The security mechanisms of the DOMAIN will be tested and validated IAW the system documentation.

Testing shall be done to assure that there are no obvious ways for an unauthorized user [REDACTED]

1.5 SECURITY CONOPS

QWEST NETWORK system security Concepts of Operations (ConOps) provides cost-effective security services to maintain protection against [REDACTED]

The QWEST NETWORK was designed and will be maintained utilizing the “Best Commercial Practices” Those practices include:

Personnel Security – While all members of the QPMO are either cleared or eligible to be cleared at the DoD Secret level. Employees who monitor and operate the QWEST NETWORK are not cleared. All Qwest employees are required to undergo a mandatory pre-employment background review, [REDACTED]

Physical Security - The major objective of Qwest Risk Management/Corporate Security is to provide a secure work environment for employees, customers and the protection of physical assets. Security’s involvement starts at the site selection process to evaluate the site and complete a risk analysis in order to assist real estate and construction in their decision on site selection. The risk analysis will focus on [REDACTED]

[REDACTED] Corporate Security will coordinate with other Risk Management groups, when appropriate, to ensure all risks to the Corporation are identified. [REDACTED]

Transport Security – Is responsible [REDACTED]

Information Systems Security - Is responsible [REDACTED]

Risk Assessment Process

- ***Trend analysis***
- ***Risk Assessment***
- ***Risk Mitigation***



Trend Analysis

Probability: What is the chance and event will occur.

Risk Assessment

Mitigation

After understanding the risks. What can be done to mitigate or lessen them?