

Appendix 2

Networx Security Plan

DRAFT

March 5, 2007

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

REVISION HISTORY	ii
TABLE OF CONTENTS	iii
LIST OF FIGURES	v
1.0 NETWORKX SECURITY PLAN	1
1.1 Purpose	2
1.2 Standards	3
2.0 Security Management Organization and Planning	5
2.1 Qwest Government Services Inc. (QGSi)	6
2.2 SAIC	9
3.0 SECURITY RISK MANAGEMENT	9
3.1 Risk Analysis standards	11
3.2 Reporting Potential Impacts	11
4.0 INFORMATION SECURITY MANAGEMENT	12
4.1 Qwest Infrastructure Security Management Architecture Features and Benefits	14
4.2 OSS Security Management	16
4.2.1 Risk Assessment	17
4.2.2 Security Test and Evaluation	18
4.2.3 Physical Security	19
4.2.4 Security Control Selection	19
4.2.5 Access Controls	19
4.2.6 OSS Security Policy	20
4.2.7 Managed OSS Security Services	23
5.0 INFORMATION ASSURANCE MANAGEMENT	26
5.1 Methods for securing OSS and infrastructure	26
5.2 OSS Security, fault and trouble management	31

6.0 SECURITY BREACH RESPONSE MANAGEMENT	35
7.0 ALARMS AND AUDIT TRAILS	37
8.0 PERSONNEL SECURITY.....	38
8.1 Qwest HR Policy/Employment Requirements	38
8.2 Access to Classified Information	38
9.0 PHYSICAL SECURITY	39
9.1 Building Security.....	40
9.2 Classified Facilities.....	40
10.0 PROCEDURAL SECURITY	41
11.0 SECURITY REFRESHMENT	42
11.1 Proactive Approach	42
11.2 Ensuring Effectiveness of controls	46
12.0 NON-DOMESTIC SERVICE SECURITY MANAGEMENT	47
13.0 FRAUD PREVENTION MANAGEMENT.....	50
13.1 Proactive and Preventative Approach	50
13.1.1 Calling Card Fraud Detection.....	51
13.1.2 Customer Premise Equipment Fraud.....	52
14.0 IMPROVED SECURITY-RELATED PROCESSES AND TECHNOLOGIES	54

LIST OF FIGURES

Figure A2-1. Qwest Risk Management Organization.....	A2-2
Figure A2-2. Laws, Regulations, and Policies Affecting Network Network Infrastructure	A2-3
Figure A2-3. Risk Mitigation Methodology	A2-12
Figure A2-4. Qwest’s Security Policy, Mechanisms and Controls, Measurements, Best Practices, Enhancements, and Certification and Accreditation	A2-15
Figure A2-5. Security Outline for Securing the OSS	A2-16
Figure A2-6. OSS Multilayered Security Model.....	A2-20
Figure A2-7. CIRT Process.....	A2-37
Figure A2-8. Technological Evolution and Convergence	A2-44
Figure A2-9. Incorporating Enhancements and Emerging Services	A2-45

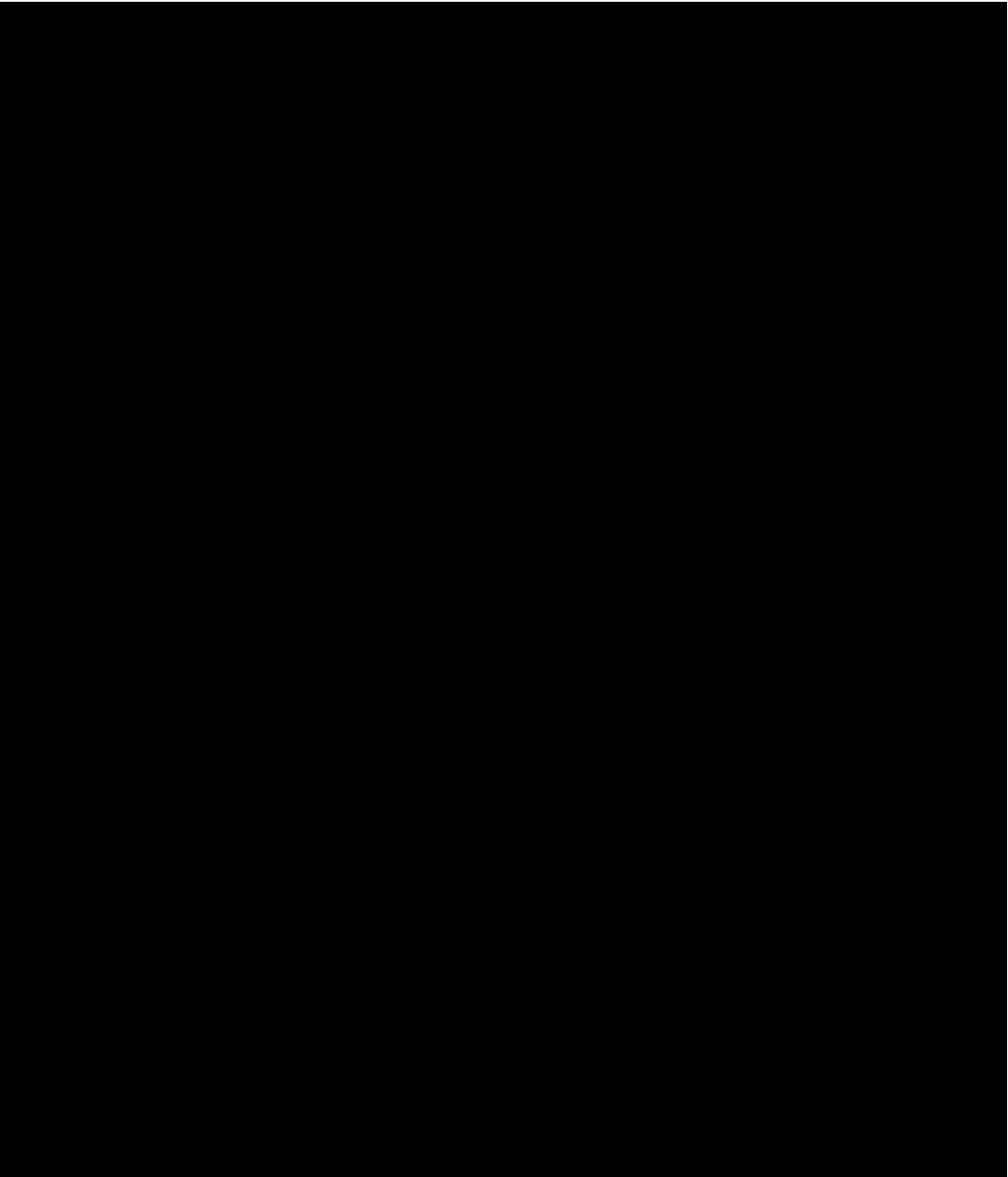
1.0 NETWORKX SECURITY PLAN

Qwest has a proven history of providing industry-leading security services to protect Qwest and our customers against threats, attacks or failures of systems in accordance with best commercial practices. Qwest is well-positioned and well-experienced to provide security-related services that ensure the integrity, confidentiality, and availability of information assets and Government information given the wide range of Networkx services, users, and geographical locations.

To protect both Qwest's and Agencies' infrastructure and information assets, we rely on an integrated risk management methodology that is comprised of a wide variety of controls for security assurance. At Qwest, security functions are organized under the integrated Risk Management Organization headed by the Vice President of Risk Management, who also serves as Qwest's Chief Ethics and Compliance Officer. Qwest's integrated Risk Management Organization [REDACTED].

Qwest [REDACTED] offers time-tested Managed Security Services (MSS) to provide options for Agencies to further secure their data and networks from threats, attacks, or system failures.

Qwest's Networkx Security Plan covers at a minimum the areas cited in C.3.3.2.4.2.1.4 and L.34.2.3.3, and will be updated as appropriate during the life of the contract in keeping with new technologies and threats. Qwest's security services meet or exceed industry best practices, and all applicable Federal Government guidelines, publications, standards, and Executive Orders (EOs).



1.1 PURPOSE

This Network Security Plan addresses how Qwest will meet the Government's information assurance standards, policies, procedures, EOs, and security controls to protect the integrity, confidentiality, and availability of

information assets for services provided to Agencies. This Networkx Security Plan includes security categorization standards for Networkx information, information systems, and the Networkx telecommunications infrastructure. The plan provides a common framework and understanding for security that, for the Government, promotes effective management and oversight of information security as it pertains to the Networkx program.

Within 30 calendar days of Notice to Proceed, Qwest will provide the GSA Networkx Program Management Office (PMO) an update to this initial draft Networkx Security Plan.

1.2 STANDARDS

The security standards identified within this Networkx Security Plan will apply to Networkx information, information systems, Networkx telecommunications infrastructure, products, and services identified within the Networkx Enterprise RFP.

The regulations, standards and policies shown in **Figure A2-2** 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 A2-2. Regulations, Standards and Policies Affecting Networkx Network Infrastructure

Regulations, Standards 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 800-18	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)

Regulations, Standards and Policies	Purpose
NIST SP 800-34	Contingency Planning for Information Technology Systems
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

Qwest's security policies are in compliance with all security control classes specified in NIST SP 800-53/Annex 1 as they relate to both the Qwest Network Infrastructure and OSS.

In addition, Qwest adheres to the following security-related standards, laws and best practices that apply to providing protection for both the Qwest infrastructure and services provided:

- eGovernment Act of 2002, Title III (Federal Information Security Management Act (FISMA))
- Office of Management and Budget (OMB) Circular A-130
- Network Reliability and Interoperability Council (NRIC) Best Practices Recommendations

- Telcordia standards
- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Processing Standards (FIPS), including FIPS PUB 200
- 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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- All applicable Qwest compliance and security standards

2.0 SECURITY MANAGEMENT ORGANIZATION AND PLANNING

Within Qwest, the responsibility for all security functions and planning is centralized as part of our integrated and enterprise-wide Risk Management

and Compliance Organization shown from an organizational perspective in Figure A2-1 above. It is led by the Vice President, Risk Management, who is also the Chief Ethics and Compliance Officer for Qwest. As a part of the compliance program, he has a clearly defined path of authority from, and escalation to, the Qwest CEO and the Qwest Board of Directors.

At Qwest, enterprise Risk Management and Compliance is organized into three main areas, all working together with a variety of operational groups, business units, and key service providers to ensure implementation of security measures including ongoing compliance management. These areas include:

- **Ethics and Compliance** (including employee Code of Conduct and Records Management functions)
- **Regulatory Compliance** Federal Communications Commission (FCC) and State Public Utility Commissions (PUCs)
- **Risk Management**
 - Safety, Environmental Affairs
 - Disaster Preparedness
 - Corporate Security
 - Information Security/Government Security
 - Claims and Insurance

2.1 QWEST GOVERNMENT SERVICES INC.

Qwest Government Services Inc. (QGSI), whose charter is to conduct business with the Federal Government, is a wholly owned subsidiary of Qwest Services Corporation.

Organizationally, Government Security falls under the Risk Management/Information Security Organization. As a team, this organization focuses on all security aspects of our Federal programs, including both

industrial security and information security. As cyber threats have grown for Agencies, Qwest has evolved our security functions to ensure close organizational alignment and collaboration among more traditional industrial security programs and technology-related functions.

Qwest has developed an integrated Networkx Security Team with the specific focus of managing all security aspects of the Networkx program. The team has dedicated a security professional to the role of the Networkx Security Manager position in the CPO. The Networkx Security Manager has the responsibility to work with the designated security points of contact within the GSA Networkx PMO and Agencies to ensure compliance with all applicable policies, publications, standards, and EOs contained in the Networkx RFP.

Qwest integrated Networkx Security Team drawing from the skill sets of the Risk Management/Information Security organization [REDACTED] will be a strong partner to GSA and Agencies, providing integrated full-service security solutions that meet the requirements of the wide range of Networkx services. The Qwest integrated Networkx Security Team has the experience necessary to adapt and grow with the Networkx program, enabling GSA and Agencies to take advantage of the security technologies and evolving Government standards and directives that provide a comprehensive security solution for Government communication challenges today and into the future.

[REDACTED] is the dedicated Networkx Security Manager. [REDACTED] [REDACTED] has over 12 years of security experience supporting various Government entities. [REDACTED] is the authorized interface with Qwest's internal organizations, suppliers, vendors, and Agencies on all security matters. Working with the Qwest Networkx CPO, he will have oversight on all activities impacting security. Working in collaboration with the Qwest Contracts Manager to ensure appropriate subcontractor compliance, Qwest's Networkx Security Manager will outline

security standards for all vendors and suppliers. The Security Manager will also document and communicate the required processes for reporting all security related issues such as escalations and violations in the Standard Practices and Procedures (SPP) Manual that will be available to all vendors, suppliers and the Government on the Qwest Control Network Portal. Qwest also have a dedicated Network Disaster Recovery (DR) Liaison Officer (for additional details on DR, please see the DR Plan in Appendix 3), as well as a dedicated Information Security Engineer. Together, with the focused effort and capabilities of Qwest's Risk Management professionals Qwest will maintain state-of-the art security practices.

Qwest's approach to communicating security policies, practices, and procedures to our employees, vendors, The Network PMO, and all Agencies to include utilization of the Qwest Control Network Portal to post relevant security policies, procedures, and reports to authorized Network stakeholders and users. These documents will be developed and maintained by the Qwest Network Security Manager. The Qwest Network Security Manager will utilize electronic mail as a means of communicating with internal staff and Government users. Emails may be either automatically generated as a notification, or authored by the Network Security Manager for specific purposes. Qwest will develop and deliver web-based security training via the Qwest Control Network Portal which will include content on network and telecommunications security, access right and privileges, acceptable use, virus protection and other additional topics. This has proven to be an effective communications tool on other Qwest Federal programs to educate employees, agents, contractors and Government users on designated security procedures related to specific activities.

The Qwest Network Security Manager along with our integrated Network Security Team will host face-to-face meetings and technology

summits with Government Networkx Security professionals to foster an enhanced understanding of Qwest's security policies and practices and to receive feedback on the effectiveness of Qwest's Networkx security practices.

2.2 [REDACTED]

Qwest has entered into a strategic business relationship with [REDACTED] to provide the Networkx MSS as identified within the Networkx Enterprise RFP.

[REDACTED] is a leading Government services contractor, with proven capabilities in designing and delivering a wide range of specific security services, technical support, and project management to Agencies such as those served by the GSA Networkx program.

[REDACTED] provides managed security solutions, networking, software development, and systems integration, as well as technical analysis and research for many Federal and State Agencies, and offers maintenance and technical support to various branches of the military. [REDACTED] also provides consulting and technology services for a variety of commercial customers. Adding this team of professionals with significant experience delivering customer-specific security services to Qwest's proven enterprise risk management program ensures a comprehensive approach to security for Networkx.

3.0 SECURITY RISK MANAGEMENT

Qwest organizations, as described above in Section 2.0, systematically identify and manage the security risk analysis processes to address infrastructure components, [REDACTED] [REDACTED] as well as the processes used to maintain them, and the environment used to deliver specific security services to Agencies. Qwest will employ a single, consistent vulnerability assessment methodology based on NIST SP 800-30 and SP 800-26, other applicable NIST standards and

contemporary industry best practices. The scope of the risk assessment will include the Qwest Control Networx Portal and OSS Applications and data. In support of Certification and Accreditation, Qwest will conduct a “self assessment” based on NIST SP 800-26 at the inception of a system and every three years thereafter as mandated by FISMA.

Qwest will conduct security control assessments of our Networx domestic/non-domestic subcontractors/vendors/suppliers. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] This approach will ensure that physical security controls are in place with Qwest's domestic/non-domestic subcontractors, vendors, and suppliers who have access to Government information. In addition, Qwest will maintain situational awareness with all subcontractors, vendors, 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.

Risk Management will work in partnership through the Qwest Networx CPO, with the Networx Security Manager, Networx DR Liaison Officer and Information Security Engineers, to ensure that Networx mission-critical information systems are managed effectively. The collaboration of Risk Management with key stakeholders from other internal organizations, such as Qwest Operations, ensures initiatives and risk remediation occur company-wide. Qwest's analysis will verify that controls selected and/or installed in support of Networx services provide a level of protection commensurate with

the acceptable level of risk. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] (See the Risk Assessment Plan, Appendix 12 to this plan, for a comprehensive overview of Qwest's Risk Analysis processes).

By using this comprehensive process, we ensure the security of services to Agencies does not degrade over time, as technology changes, systems evolve, or people and procedures change. This ongoing review process provides assurance that management, operations, personnel, and technical controls remain in place, providing adequate levels of protection through the life of the program.


3.1 RISK ANALYSIS STANDARDS

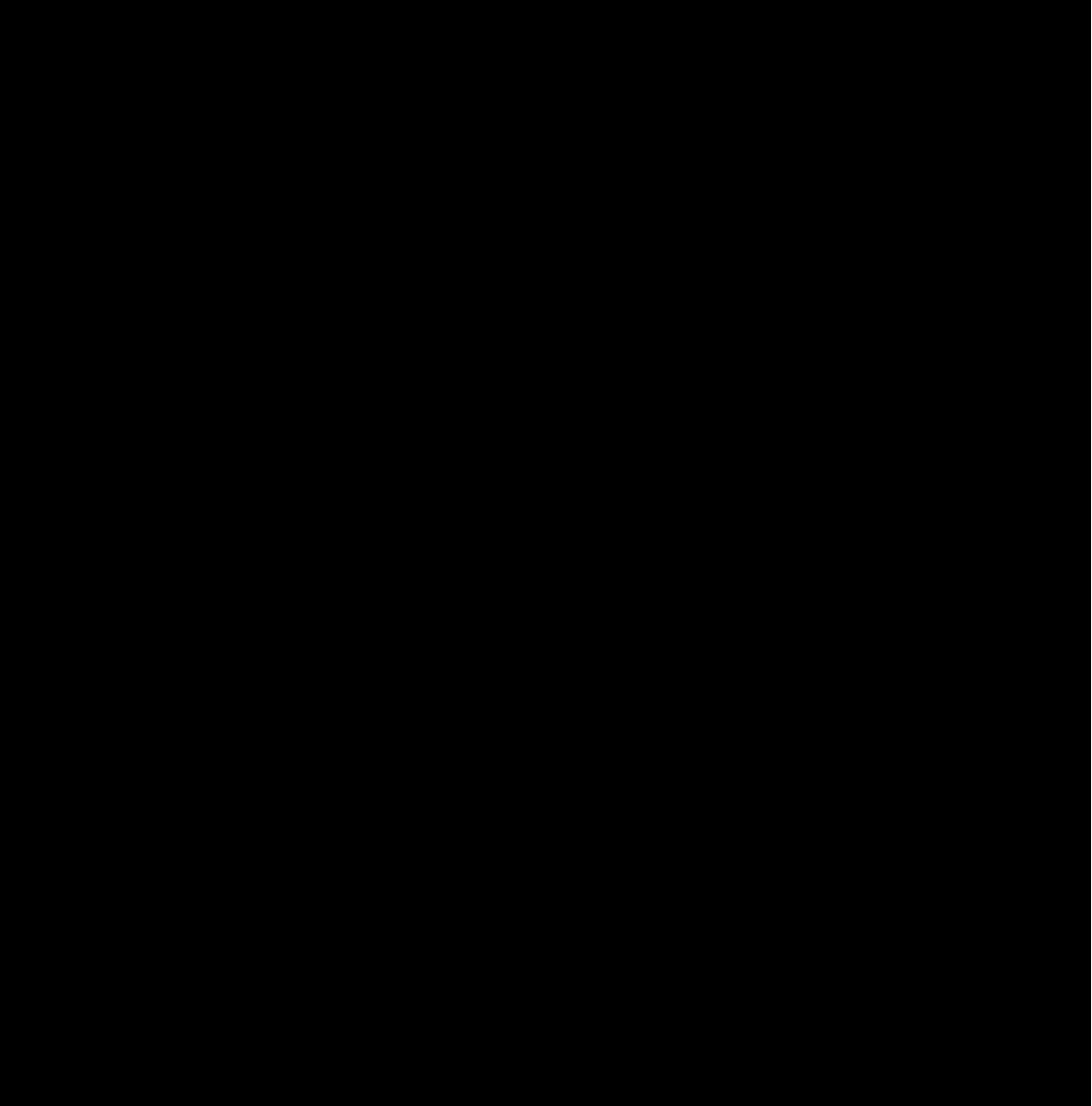
All security risk analysis activities will adhere to the following:

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

3.2 REPORTING POTENTIAL IMPACTS

Working with Agencies, 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 and categorization definitions to all Networx security risk assessment reports and activities. The application of these definitions must take place within the context of each organization participating in the Networx program for the overall national interest.

 Qwest risk mitigation methodology used throughout the Networkx Security Risk Analysis process.



4.0 INFORMATION SECURITY MANAGEMENT

Securing the Qwest infrastructure – whether within corporate environments, Agency-facing networks, or the administrative infrastructure that links them – requires collaboration for risk assessment, policymaking, threat remediation, and implementation of best practices. Qwest information

security-related functions are performed in close collaboration with Qwest's Operations organizations [REDACTED]

[REDACTED]

To ensure all security-related events with a potential impact to Agencies are identified, handled, and communicated in a timely manner, this information will be coordinated through the Qwest Networkx Security Manager.

Qwest ensures the integrity, confidentiality, and availability of Government information and data that is transported on the Qwest infrastructure. Qwest-owned services that transport and/or store Networkx information and data comply with NIST requirements for security plans in SP 800-18 and controls as specified in FIPS 200 and SP 800-53 within the Networkx system boundaries as specified by SP 800-18, based on the systems impact designation as specified by FIPS 199. All Qwest-owned services applied to Networkx information and data will comply with the requirements of FISMA and the certification and accreditation criteria in SP 800-37. Qwest will provide the system security documentation to Agency and Agency-designated auditors as required to maintain the system's Certification and Accreditation status.

4.1 QWEST INFRASTRUCTURE SECURITY MANAGEMENT ARCHITECTURE FEATURES AND BENEFITS

████████████████████ the scope of the Qwest infrastructure security management architecture features and benefits under the following framework:

- **Qwest Security Policy:** Provides a comprehensive view to support the entire spectrum of Federal requirements
- **Mechanisms and Controls:** Entails comprehensive processes that support protection from a full spectrum of security risks, ensuring continuous delivery of high quality secure services
- **Proven Measures:** Proven applied set of techniques that implement and enforce security policy which ensures continuing delivery of high quality secure services
- **Proven Best Practices:** Application of the Qwest approach lowers risk to Agencies
- **Enhancements:** Eliminates potential barriers of evolution toward converged Next-Generation services
- **Certification and Accreditation:** Mature, proven ability to establish security compliance facilitates service delivery

4.2 OSS SECURITY MANAGEMENT

Qwest's single comprehensive Networkx Security Plan includes all Qwest Networkx components as determined by the FIPS 199 security categorization and based on NIST SP 800-18. The goal of the plan is to ensure the three security objectives of confidentiality, integrity and availability across the proposed Networkx services including the safeguards that implement those objectives. The plan will include the Qwest Control Networkx Portal and OSS. Qwest will define and develop the required controls for physical, logical and managerial functions based on NIST SP 800-53, FIPS-200 and contemporary industry best practices for each Networkx component based on its individual security impact. The Qwest Networkx Security Plan will be revised as required, so that Certification and Accreditation activities may begin with the Government's Notice to Proceed. The Qwest Networkx Security Plan includes contractual controls to ensure strict supplier, subcontractor, and international vendor compliance with all Federal security standards and requirements. Qwest will manage the security of the OSS, databases, and information systems in accordance with guidance contained in Federal Information Security Management Act (FISMA); implementation of National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), or other applicable Federal or Agency requirements. Qwest will secure the OSS by implementation of the Operational, Technical, and Management controls [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

1.0 System				
[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]

As an integral part of the Security Management Team an Information Assurance Officer (IAO), Information System Security Manager (ISSM) and Security Manager will enforce all security polices and procedures associated with OSS as listed in Figure A2-5 and other applicable Agency directives, FISMA, NIST, or Congressional mandates. The purpose of these policies is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall information system security policy, evaluation and approval/accreditation NIACAP responsibilities promulgated by NIST Standards and applicable Federal or Congressional directives.

4.2.1 Risk Assessment

The Qwest Security Management Team has conducted risk assessment in accordance with NIST SP 800-50, and Qwest best practices

on the OSS and its environment to evaluate and assess the threat environment in terms of Security Impact and Security Objectives of the OSS and its applications. From this assessment, Qwest has developed the appropriate security controls and countermeasures to meet the threat environment.

Security Objectives describe the security paradigm of the security apparatus required by FISMA; these form the basis for our measures, and there is a direct correlation between confidentiality, integrity, and availability of the OSS in terms of mission impact (low-impact, moderate-impact, or high-impact) and the appropriate security controls levied against it.

The Risk Assessment of the OSS information technology includes physical and logical resources (e.g., access, facilities, installations, personnel, equipment, transmissions, emanations, electronic media, and documents).

The security controls as described in the Section 3.13 of the Qwest proposal along with Section 5.1 of this Networx Security Plan are applied in accordance with NIST 800-53 and FIPS Publication 199/200 to meet the applicable Security Category.

4.2.2 Security Test and Evaluation

Qwest, through a third-party independent tester, will execute the Security Test and Evaluation (ST&E) Plan against operational, management, and technical security controls and procedures to validate the security controls implemented on the OSS for Designated Approval Authority (DAA) Certification and Accreditation Authorization to Operate (ATO) in accordance with NIACAP. Qwest will provide the technical analysis of the raw data results from the execution of the ST&E Plan and procedures and the automated tool(s). A third-party independent tester will write the test report, document the results, and provide any technical narrative that may be required in support of any Certification and Accreditation activity. Qwest will support site

security assessment visits and operational testing as required. Qwest will document security related findings and recommendations from the ST&E Plan and provide remediation, mitigation, and action plans as required by DAA.

4.2.3 Physical Security

Physical security is the action taken to protect OSS information technology resources (e.g., access, facilities, installations, personnel, equipment, electronic media, documents) from damage, loss, theft, or unauthorized physical or passive access through the security controls that Qwest has implemented as stated in Section 5.1. Qwest will ensure physical security is in accordance with DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM) and the Networx Enterprise RFP.


4.2.4 Security Control Selection

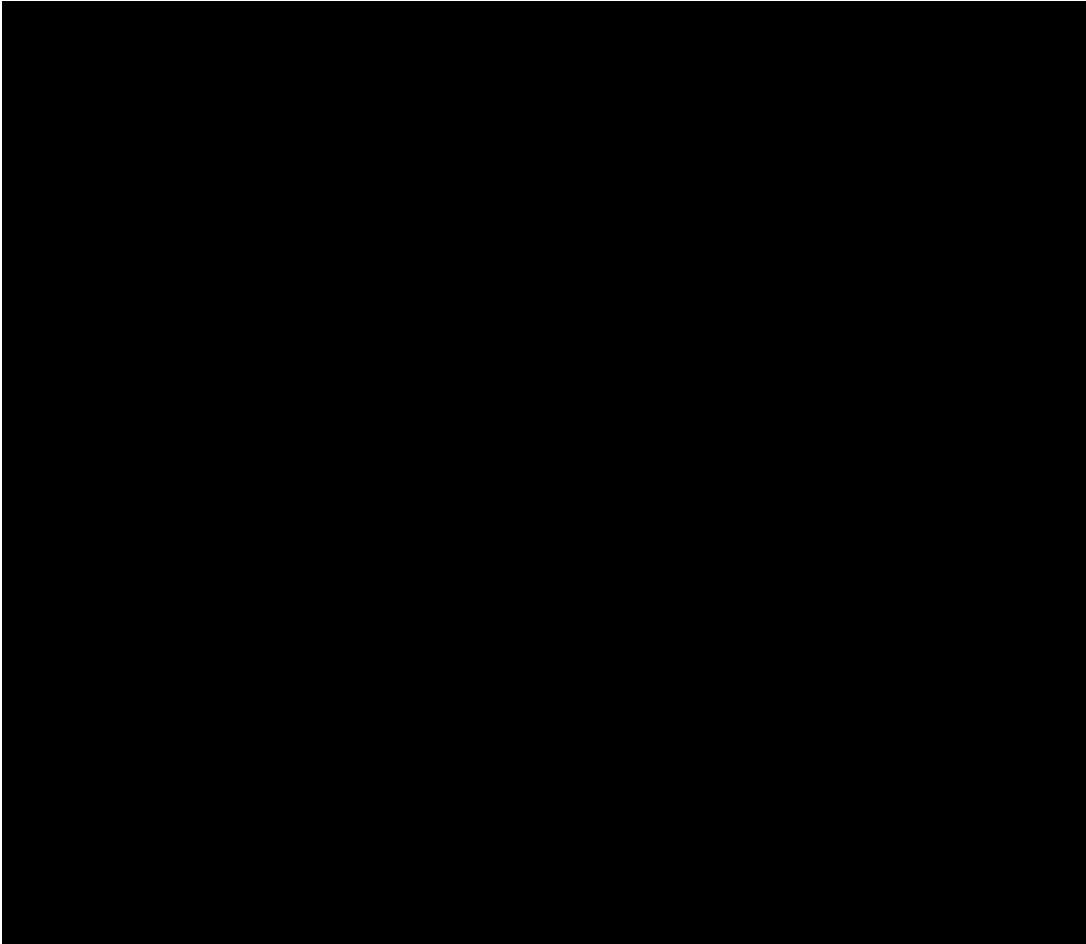
Qwest OSS meets the minimum security requirements for security controls and assurance requirements in accordance with FIPS Publication 199/200, NIST Special Publication 800-53 and Qwest best practices. The selection of the appropriate security controls for the OSS is a risk-based activity involving management and operational personnel within the Qwest organization, and will be conducted in accordance with FIPS Publication 199/200.

4.2.5 Access Controls

Security policies are defined and enforced for the OSS in accordance with Annex 2 to NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems Minimum*. Appropriate baseline security controls have been implemented for access to the OSS, or components within the OSS, in order to protect the OSS from unauthorized access.

4.2.6 OSS Security Policy

To ensure security of the OSS, Qwest is deploying a multi-layered security model  employing appropriate software and hardware, to implement management, operation and technical controls at each successive layer. These countermeasures and controls ensure the security of the OSS. Additionally, the integrated Networx Security Team has implemented security measures as shown in Figure A2-6 for management of daily OSS operations.



4.2.6.1 Security Policy/Discretionary Access Controls

Qwest understands the need to ensure that strong measures are in place to manage identification, authentication, and authorization for those personnel involved in providing Networx services, especially technicians who access network elements and routing policies, and require access to network management and other systems that may include Agency-related information. Qwest uses access controls and other methods as described in Section 5.1, Methods for Securing OSS and Infrastructure, to manage use of systems and infrastructure.

Access to the OSS will be controlled by Access Control Lists (ACLs). All personnel that have access to the OSS will have proper authorization based on need-to-know. Discretionary access controls are required such as user ID and password in accordance with Qwest directives to ensure that only selected users or groups of users may obtain access to the network based on clearance and the need-to-know.

The OSS access controls will be capable of including or excluding access to the granularity of a single user or a group of users. The OSS controls will provide authentication, access control, auditing identification, and accountability.

4.2.6.1.1 Identification/Authorization

Individuals that have access to the OSS must be identified. Access is restricted by classes of information that individuals are authorized to access as per the ACLs. The identification/authorization information will be securely maintained by the system that will perform security action.

4.2.6.1.2 Accountability

The OSS will have the capacity to protect the audit trail from modification, unauthorized access, or destruction of the objects it protects. In order to protect audit information, the OSS will allow access only to personnel

authorized to audit the information. The OSS will be able to record events such as identification and authentication, file open, program initiation, deletion of objects, actions taken by users (e.g., computer operators and system administrators) and all significant system events. For each recorded event, the audit record will identify the 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 and terminal ID will be included in the audit record. The OSS administrator will have the capacity to audit the actions of users based on individual identity.

4.2.6.1.3 Personnel Security Policy

All personnel that have access to the OSS will have proper authorization. Discretionary access controls are required to ensure that only selected users or groups of users may obtain access to data based on clearance and the need to know.

The OSS will contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements. In order to assure that the four requirements of Authentication, Access Control, Auditing Identification, and Accountability are enforced by the OSS, there must be some identified and unified collection of hardware and software controls that perform these 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 adequacy.

OSS administrators will develop 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. Qwest's OSS administrators will provide controls to

limit access rights based on level of clearance and the need-to-know. Qwest Information Systems has developed the Controlled Access list using the ██████████ Controlled Access protection model which will be applied to the administrative portal in accordance with NIST 800-53, Annex 2.

Access controls on the OSS will have the capability of including or excluding access by a single user. Only Network Administrators may assign access. Limited access rights will be based on level of clearance and the need to know.

ACLs will be kept current and will be updated in accordance with Qwest Standards when required due to employment termination or reassignment.

4.2.7 Managed OSS Security Services

Qwest will provide security within the infrastructure of the OSS against threats from hacker, criminal, and terrorist activities, using methods consistent with commercial practice, and that ensure availability of service, confidentiality, and data integrity of transmission and switching systems, support systems, and databases being maintained by Qwest in support of the services. Qwest will monitor potential security problems on a 24x7x365 basis.

4.2.7.1 Management of Qwest Control Networx Portal System

Qwest will provide and maintain a user-friendly, secure, Web-based interface to the OSS and its associated service delivery support systems, via the Qwest Control Networx Portal. This system will enable the Government to easily order, track, and review the status of all services. Qwest integrates a wide array of data sources into a single secure Web-based interface.

Qwest will provide all hardware, software, integration, and support necessary for the Government to interface with the Qwest Control Networx Portal. Qwest will maintain the Portal so that the Government can access data, configuration diagrams, and reports. Qwest has incorporated several

Actuate tools for additional ad hoc reporting queries into a variety of Qwest databases.

Qwest will provide for the protection of Sensitive But Unclassified (SBU) communications commensurate with FISMA and NIST 800 standards. Qwest will secure and maintain the protection of the Portal at the facility locations where Qwest has proposed to install applicable equipment.

Qwest will follow NIST and FISMA guidance, and Qwest best commercial practices to protect its sensitive systems. These sensitive systems include but are not limited to databases, critical subscribers' locations, identifications, authorization codes, and call records. These sensitive systems may also include computer systems that control the Qwest Control Networx Portal.

Qwest will provide security within the infrastructure of the Qwest Control Networx Portal against threats from hacker, criminal, and terrorist activities, consistent with commercial practice. Our security practices will ensure availability of service, confidentiality, and data integrity of the Portal transmission and switching systems, the support systems, and the databases being maintained by Qwest to support Networx services. Only authorized Government personnel, as determined by the Government, will have access to those portions of the Portal based on their need to know.

4.2.7.2 Contingency Planning

The Qwest OSS Contingency Plan outlines planning principles designed and implemented in response to incidents that could adversely affect system operations. Conversely, OMB Circular A-130 requires continuity of operations planning for every information system. The Qwest OSS Contingency Plan includes both contingency and continuity planning.

The OSS Contingency Plan identifies process-planning requirements and develops contingency plans in the case of disaster or prolonged outages.

The OSS Contingency Plan is developed in accordance with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems and also meets the requirements of the Department of Homeland Security.

The OSS overall risk management program must cover Qwest's ability to respond to unplanned, adverse situations that may destroy, damage, degrade, or compromise information systems data or computer processing capabilities so that essential operations may continue. Ensuring that this ability exists, and is indeed viable (proven via periodic testing), is the major function of continuity of operations planning.

To avert disruptions, or minimize their damage, organizations must take proactive steps to develop the Continuity of Operations Plan (COOP). The Contingency portion of the COOP focuses on minimal, day-to-day outages (server down, localized short-term connectivity loss, etc.), while the Continuity portion deals with long-term or disaster scenarios. The COOP contains operational recovery issues, ranging from arrangements for a limited backup capability (needed files, programs, paper stocks, pre-printed forms, etc.) to relocation to a different facility in the event of a total failure. The goal is to protect lives, limit damage to property, and minimize the impact on operations, including information systems processing activities.

4.2.7.3 Security Services

[REDACTED]

[REDACTED]

5.0 INFORMATION ASSURANCE MANAGEMENT

To safeguard critical services, including all Networkx services, Qwest infrastructure and the OSS environment, against cyber attacks, Qwest has deployed a variety of measures to prevent or minimize the impact of any possible disruptions. Upon notification from the GSA Networkx PMO, the integrated Networkx Security Team will ensure that any additional information assurance measures required to support Networkx are included.

5.1 METHODS FOR SECURING OSS AND INFRASTRUCTURE

The pre-existing processes used within the Qwest infrastructure, where “infrastructure” encompasses the Networkx services and the OSS, include, but are not limited to the following controls:

- **Configuration Management Controls:** Ensure network element configurations and software images conform to vendors and industry best common practices and recommendations. [REDACTED]

[REDACTED]

- **Patch Management:** The Qwest Team will provide patch management services on Qwest Control Networx Portal workstations, servers, routers, OSS, and network elements throughout the life of the Networx program. Patches will be installed at the earliest possible opportunity commensurate with the nature of the threat/issue and risk to the Qwest Control Networx Portal. For non-critical issues, patches will be tested in a lab environment and, upon acceptance, deployed to the production environment at the next change management window. For critical patches, [REDACTED]

[REDACTED]

Program Office for the affected systems. In the event issues are identified in the lab concerning deployment of the patch, Portal mitigation options and countermeasures will be researched and the observations/findings coordinated with appropriate GSA and Agency offices.

- **User and Protocol Access Controls:** Restrict access to the management and control planes of the network elements including use of encryption and two-factor authentication methods. Rate limiting and blocking of protocols directed specifically to the network elements along with blocking of management and control plane traffic to network elements from untrusted sources provides further protection.

- **Network Architectures:** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

- **IP Spoofing Prevention Measures:** Include implementation of anti-spoofing technologies on the majority of our edge and border routers to prevent spoofed network attacks from entering the Qwest network [REDACTED]

[REDACTED]

- **Comprehensive Monitoring and Alarming of Infrastructure**
Components: Provide real-time monitoring of network elements with alarm notifications to the Qwest Network Management Center (operating 24x7x365) and rapid response to events that may indicate a security issue utilizing standard processes, tools, and techniques as described in Section 3.2, Network Management.

- **Denial of Service and Distributed Denial of Service (DoS/DDoS):**
Monitoring and mitigation measures include flow monitoring across our border routers to provide proactive attack identification and mitigation; Qwest and Agency-initiated IP address [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- **In-Depth Certification Testing:** Ensures comprehensive hardening, testing and ongoing auditing of the network elements including routers, switches and servers.

- **Robustness and Failover of IP Traffic and Backbone Services:**
Provides rapid recovery and minimal Agency impact from events using techniques and capabilities such as: [REDACTED]

[REDACTED]

[REDACTED] systems that provide a highly, geographically redundant, DNS service; redundant router and circuit links in each point of presence; and additional capabilities currently under development, including

[REDACTED]

- **Virus Protection Controls:** Anti-malware/anti-spyware controls are incorporated at multiple layers in the Qwest infrastructure. We accomplish this mission via clear standards-setting, and a vendor-diversity strategy to ensure the timeliest response to new threats and well-defined, operationalized incident response procedures. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Virus pattern updates are pushed out to the users using regularly scheduled, automated techniques that can be executed more rapidly in times of emergencies, ensuring the latest viruses are recognized and deleted. On email systems connected to the Internet, content scanning on incoming and outgoing email messages for malicious code is also conducted, with real-time updates for virus pattern files along with an aggressive file attachment blocking strategy. Finally, Instant Messaging services are tightly controlled, limited to specific business purposes, and active content such as files and URLs are not permitted from external sources.

- **Logical Perimeter Security and Intrusion Detection/Prevention**
Techniques: Ensure that Qwest infrastructure is protected from Internet-borne threats or unauthorized access through our network connection points, and include a variety of firewall, intrusion detection, prevention, and other protective controls including two-factor authentication for remote access users.

- **Standardized Identity Management:** Controls ensure that all those who access Qwest systems are granted unique identifiers and given access only to those systems for which they have a specific business need to access. In addition to this least-privilege model of security, Qwest also employs two-factor controls, such as tokens and digital certificates for access to critical elements and remote access to our networks. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] are restricted to authorized users with access based on demonstration of a specific business need to know (least-privilege model). The policies and standards governing the appropriate use of security credentials, including the rules for requesting, granting, authorizing, approving, using, resetting, modifying, revoking auditing, and deleting credentials and passwords, are owned by the Information Security organization.
- **Access Controls:** Qwest employs a variety of controls within the OSS environment, including access controls that operate within the framework described above as Standardized Identity Management. Agency access to the OSS for service ordering and other functions is also controlled as detailed in Section 3.13 OSS, to assure that only appropriate Agency contacts are permitted access to the OSS functions and data. These controls also limit visibility of the data provided to all Agency contacts according to the contact's function and authority as defined by the authoritative Agency contact (administrator).
- **Network Elements Controls:** Operating within the Standardized Identity Management controls as described above, Qwest secures our network elements and other infrastructure components using both logical and

physical measures including, but not limited to [REDACTED]
[REDACTED]
[REDACTED] limit the visibility of elements. Only those operational employees with specific need to access elements are provided with credentials, and credential management processes include specific standards for adding, changing and deleting as well as periodic audit of access credentials. These audits review credentials to ensure only current, active, appropriate individuals are able to access network elements. Finally, these access control processes also include limiting privilege levels on elements to only those required to meet specific service and business needs.

In addition to the above mentioned controls, Qwest also utilizes an internal Security Evaluation process to review new applications, infrastructure components (elements) and products for adherence to security standards prior to deployment as well as ongoing security assessments of existing infrastructure – including Networx services, Qwest infrastructure, and the OSS environment – to identify security vulnerabilities and remediate them in a timely fashion.

5.2 OSS SECURITY, FAULT AND TROUBLE MANAGEMENT

Qwest will meet the requirements for security management, fault management, and trouble handling for OSS in compliance with the Networx RFP.

Qwest has a robust security incident and resolution process providing 24x7x365 call coverage to receive, report, and assist with security incident calls to maintain a reliability factor of [REDACTED] percent availability of the Qwest Control Networx Portal and its features. Qwest will provide the capability for Agency or Qwest personnel to report security incidents to the toll-free phone

line to the Secure NOC. In addition, the Portal will incorporate the capability to report, track, and manage security incidents. The availability of this capability overlaps the Agency business hours defined as Monday through Friday, 7:00 a.m. - 7:00 p.m. Procedures for security incident support and resolution will be consistent with requirements specified by the Agency and the Incident Response Plan. Qwest understands that resolving some security incidents will require action on the part of the Agency; therefore, no timeframe parameters are specified. Qwest will report all such detected security incidents within 15 minutes to the Networx PMO and all affected Agencies. The Qwest Secure NOC will cooperate with the Agency to mutually agree to a timeframe for resolution of each security incident, depending on the nature of the incident. Qwest will report on the results of the investigation and corrective measures applied to the security breach or problem within four hours of notifying the PMO and Agencies that a security breach, violation, or problem has occurred.

Any delays or hindrance in resolution will be escalated and reported to the Agency COTR, security manager, or designated POC in accordance with the Government's escalation process. The Qwest Secure NOC will continuously monitor for service degradation and network component alarms which includes monitoring for security incidents.

Fault management is maintained by Qwest's Network Management organization and is focused on network reliability and performance to reduce the frequency, severity, and duration of fault events. Qwest proactively manages our network, using state-of-the-art tools and operational processes that help make us a leading provider of telecommunications and data services. GSA and Agencies will have real-time access through the Qwest Control Networx Portal to obtain the latest information regarding network faults. Qwest will manage the reliability of our network and that of our team

members in real-time, with Agency controlled access through the Portal for application use. In addition, Qwest uses state-of-the-art communication tracking and development tools for proactive monitoring of events, traps, and alarms to ensure network integrity. Qwest's goal is to minimize any down-time, service dispatches, or repair issues. Through our inherent systems and our Networx team members, Qwest will isolate and resolve issues before they impact service. Our goal is simple: Qwest will work toward ensuring our network is always at optimal operating levels.

Qwest's trouble handling is managed through secure systems and processes. Most troubles will be proactively identified and resolved prior to any impact to Agencies through our network management system's advanced surveillance system. Alarm thresholds will be set to trigger prior to Agency-apparent services degradation. Qwest will take all necessary corrective action to ensure continued service quality. For other troubles, prompt contact to the Qwest CSO will enable our technicians to quickly respond, engage, and commence the troubleshooting process. Agencies will receive timely status on the progress and corrective action taken to resolve a trouble. For complex issues, Qwest's established process will engage the required technical expertise for prompt trouble resolution, up to and including Tier 3 industry subject matter experts.

In addition to the extensive controls that Qwest employs within our infrastructure, Qwest's managed security services include the following additional security controls to safeguard critical services to the Agencies:

- The Qwest **Managed Firewall Service** (MFS) provides a comprehensive management service, delivering three levels of tiered service, a multitude of value-added features, and a robust offering of Service Enabling Devices (SEDs) to meet the requirements of Agencies.

- With Qwest's **Intrusion Detection and Prevention Service (IDPS)**, Qwest offers Agencies effective systems and processes to: monitor their networks for attacks, misuse, and anomalies; detect and record such intrusions; and begin immediate corrective responses.
- The Qwest **Vulnerability Scanning Service (VSS)** allows Agencies to conduct effective and proactive assessments of critical networking environments, enabling the rapid correction of vulnerabilities before they are exploited.
- The Qwest **Anti-Virus Management Service (AVMS)** provides detection and removal of system viruses before they can do critical damage to business operations.
- The Qwest **Incident Response Service (INRS)** provides incident response capability assessment, an incident tracking system, a mock crisis management scenario, incident response support services, and on-site support.
- The Qwest **Managed E-Authentication Service (MEAS)** offering provides design, implementation, and operational capabilities for both token-based and certificate-based e-authentication services in a variety of hosting and operational environments. We also offer significant capabilities in identity management, access control, and biometrics.
- The Qwest **Secure Managed E-mail Service (SMEMS)** will provide Agencies with the ability to centralize and assure inbound and outbound email policy compliance, ease of administration, ability to meet legal and regulatory requirements on email retention, security/privacy (via a patented pass-through process, not store-and-forward), and ability to leverage the cost effectiveness of the Internet while providing

confidentiality, integrity, and availability of email services that are expected by Agencies.

- The Qwest **Managed Tiered Security Service** (MTSS) offering provides Agencies security solutions that can be customized for specific Agencies, based on the respective level of mission criticality and information sensitivity.

Qwest service offerings across all of the Networkx service categories include their own, specialized controls, to protect Agency information. Qwest can also offer Agencies a customized set of technical controls to ensure a strong security posture. Qwest Networkx team members are experienced in applying these products and services to specific Agency situations.

6.0 SECURITY BREACH RESPONSE MANAGEMENT

In the event that there is a security breach, Qwest will use a multi-pronged approach to meet a variety of technology scenarios depending on the location, Agency infrastructure or Qwest infrastructure, of the detected security-related alert or event. Regardless of the event's source, the Qwest integrated Networkx Security Team will ensure that all incidents are reported within the required time frame, including: a verbal notification to the GSA Networkx PMO and affected Agencies within fifteen minutes for initial discovery, and within four hours for results of investigations and corrective measures applied; a written Security Breach Notification Report within seven calendar days of said breach; and a monthly report detailing all security breaches for that month.

If a security breach is detected in the Agency infrastructure, those breaches will be detected by the Secure Operations Center (SOC) via the specific security services. The SOC will work in coordination with the Networkx Security Manager and the Agency or Agencies involved, following established

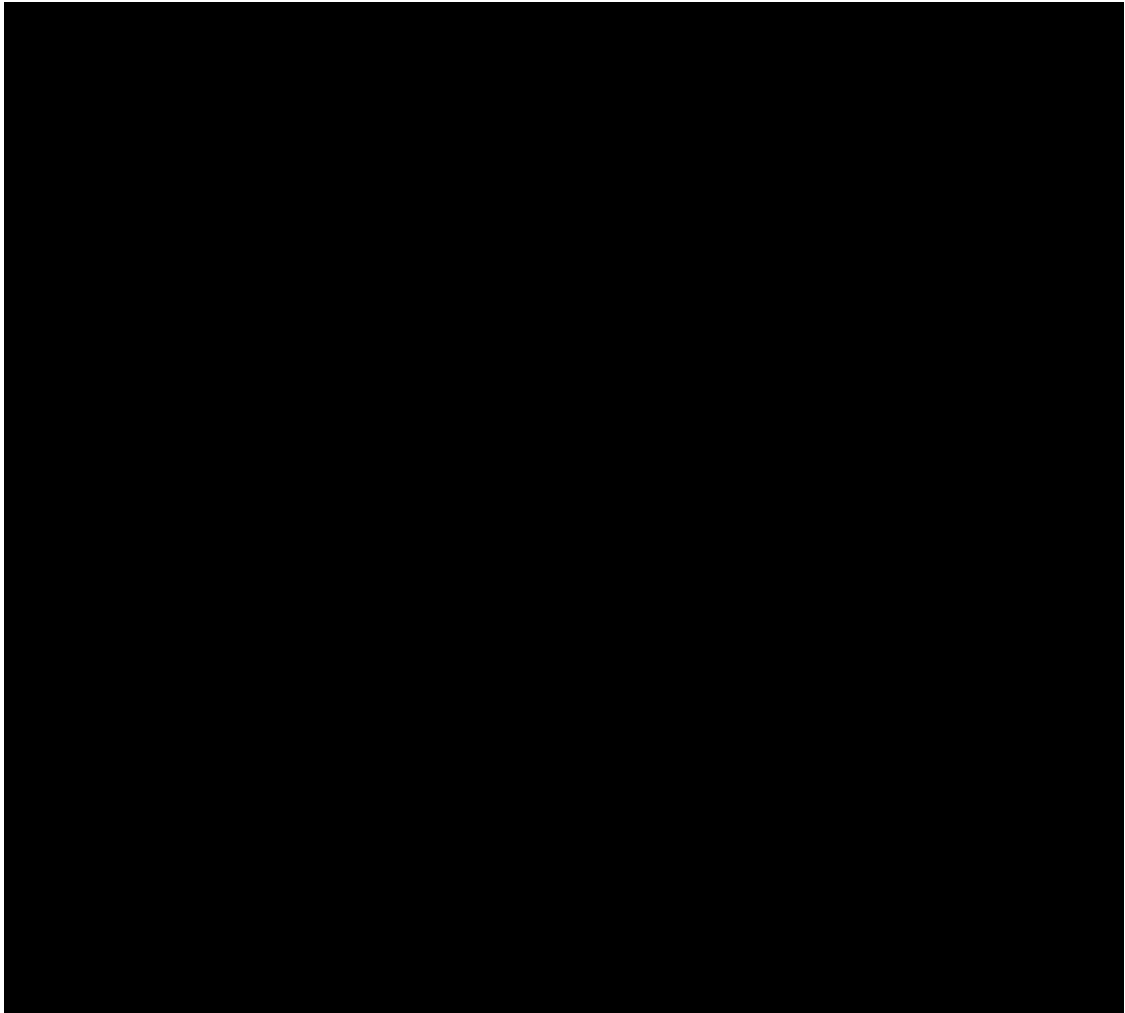
escalation and reporting mechanisms. Depending upon the types of security services utilized under the Networx contract by the Agency or Agencies, follow-up and remediation activities will commence.

If the Agency decides to engage law enforcement, Qwest will provide subject matter expertise and any Agency-specific data that is required.

If a security breach is detected within the Qwest infrastructure, it will be managed by the corporate-level Cyber Incident Response Team (CIRT), as documented in the CIRT – Response Process [REDACTED] which includes internal formal process documents, training, and response integration with overall corporate Emergency Response Team (ERT) processes and with specific operational functions as a part of our integrated Risk Management and Networx program team.

Notifications will be made to Operations, detailing range of impact (event or mitigation/remediation driven), risk level and Qwest exposure, and any requirements for additional technical resources. At the same time, depending upon the severity of the CIRT event, Senior Qwest Management may be engaged. An assessment is made for the need of communicating internally and externally to various Agencies, Telecom-ISAC and other external communications points.

The Qwest Networx Security Manager will be notified and will be responsible for coordinating communications and follow-up for all Networx impacting events. In the case where the notification is a security alert, Qwest will follow its SecAlert process and the ERT structure will be activated.



7.0 ALARMS AND AUDIT TRAILS

Qwest's comprehensive monitoring and alarming of infrastructure components provides real-time monitoring of network elements with alarm notifications to either the Qwest NOC for Qwest element-related events or the SOC for Agency-related events. Both are staffed 24x7x365, and provide rapid response to events that may indicate a security issue utilizing standard processes, tools, and techniques as described in Section 3.2, Network Management.

Qwest implements a standardized approach to generating alarms and audit logs for specific events, including those with potential security impact.

Detailed implementations are attuned to specific network and computing technologies and the potential risk associated with individual elements, both for services and security-related issues. Audit logs (trails) are examined on a regular basis, and retained according to specific operational procedures. Qwest Risk Management drives investigations including post-event examination of logs in cases where there may be signs of potential misuse or abuse, and Operations groups have specific log examination and review schedules as a part of their ongoing network management procedures.

The Qwest Network Security Manager will work with the Agencies to ensure any specific requirements for alarms and audit trails within the Qwest infrastructure are met, while Agency-specific alarming and auditing strategies will be developed as a part of the deployment process for security.

8.0 PERSONNEL SECURITY

8.1 QWEST HR POLICY/EMPLOYMENT REQUIREMENTS

[REDACTED]

8.2 ACCESS TO CLASSIFIED INFORMATION

If security clearances are required to access classified information in support of the Network Program, Qwest's Personnel Security Manager (PSM), located at Qwest's cleared facility [REDACTED] [REDACTED] will process the employee clearances in accordance

with the requirements set forth in the Department of Defense Contract Security Classification Specification (DD Form 254). Qwest will flow down to [REDACTED] or other subcontractors any requirements for clearance processing for their employees to support Networkx.

Security clearances will be based on the level of security defined by the Agencies. A request for a security clearance will be submitted only for those employees who require access to classified information in the performance of a task or service essential to the fulfillment of the Networkx program. Qwest's PSM, who reports to the Director of QGSI Security, is responsible for assisting the employee with proper completion of [REDACTED] [REDACTED] and submitting the completed paperwork to the Office of Personnel Management (OPM) for processing.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

9.0 PHYSICAL SECURITY

Qwest will ensure the integrity, confidentiality, availability, and protection of Government information and data that is handled manually at Qwest-owned facilities, in accordance with FIPS 199 designation of low, moderate or high security level with appropriate documentation of compliance. All Qwest staff with access to Networkx information and data will have the appropriate level of background investigation with documentation provided to the Government as required.

9.1 BUILDING SECURITY

Within Qwest Risk Management, Corporate Security has a Physical Security Group that establishes security policies, manages access control systems, and coordinates security improvements to Qwest properties. Physical Security evaluates each prospective facility site, and completes a site survey in order to assist real estate and construction in site selection. The site survey focuses on the types and levels of potential threats, the criticality of the site, and other factors that impact security. Once a site has been selected, Physical Security will perform a formal risk analysis and make recommendations on site design, perimeter physical security measures, and the installation of appropriate electronic security systems. Qwest supports a robust program of physical security measures, including a variety of standardized facility controls such as [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] perimeter security approaches such as fencing, gating, and lighting.

Qwest's integrated Networx Security Team will work with Physical Security to identify any spaces to be used in support of the Networx program. Physical Security will use Qwest's [REDACTED] [REDACTED] to provide the baseline requirements.

9.2 CLASSIFIED FACILITIES

The Qwest integrated Networx Security Team has extensive experience in NISPOM requirements for accreditation of classified facilities, and has nominated an experienced security professional to be the Networx Security Manager.

QGSi currently has three cleared facilities from which classified activities for Networkx will be supported. [REDACTED]

[REDACTED]. Qwest will work with the GSA Networkx PMO to obtain the required accreditations at the appropriate level, to support any classified tasks for Networkx as defined in the DD254.

10.0 PROCEDURAL SECURITY

Qwest will comply with the mandates of the Federal Information Security Management Act (FISMA) of 2002, with respect to the services provided. NIST created the 800 series of Publications, including Special Publication 800-14 to provide guidelines on security controls for Federal Information Systems.

To ensure Agency compliance with these obligations, Qwest's integrated Networkx Security Team will implement strategies and processes to assure service levels, policy compliance, and appropriate risk management to secure all assets and services.

Qwest is providing to Networkx award-winning, industry-recognized products that can dramatically enhance the protection profile of Federal Agencies, and aid Chief Information Officers (CIOs) in complying with the requirements detailed in NIST SP 800-53. Qwest's integrated Networkx Security Team will specifically aid Agencies in the areas of:

- **Performance and Availability Management** – Monitoring, managing, and reporting on service levels, application performance, and systems capacity
- **Security Management** – Identifying, tracking, and resolving security incidents in real time

- **Operational Change Control** – Ensuring changes are properly authorized and tested off-line before they are placed into production protecting sensitive databases and information
- **Configuration and Vulnerability Management** – Auditing and enforcing system compliance with organizational configuration policies

11.0 SECURITY REFRESHMENT

11.1 PROACTIVE APPROACH

Qwest understands that the dynamic nature of the threat climate along with the continual stream of published vulnerabilities calls for a proactive, process-oriented approach to continuous improvement in the Qwest security posture for all infrastructure components. These infrastructure components include, but are not limited to, all Networkx services, Qwest infrastructure and the OSS environment, including databases and configuration changes. Through a multi-pronged approach, Qwest keeps apprised of the latest threats, modern security measures, and the latest trends, methods, and technologies for preventing and detecting security breaches that will continuously improve the overall Networkx security throughout the life of the contract. Key elements of the Qwest approach include, but are not limited to, the following:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

These relationships are also vital to the Networkx program and Agencies as technology continues to evolve, since such technology change and convergence can bring additional risk if transitional periods are not managed effectively. The Qwest environment minimizes the risk during these times of technology change and evolution by providing for interoperability. This approach ensures a smooth transition to new technologies while providing stability and security. This approach provides Agencies with the best defense against denial-of-service attacks, intrusions, and other perceived threats, by leveraging new technologies and features.

Network architecture is also applicable to Qwest's proactive approach to security, as evolving technology supports interoperability and thus a more secure environment. [REDACTED]

Utilizing the Qwest Networkx Security Manager as a single point of contact, Qwest will review with the GSA Networkx PMO and Agencies any network security enhancement notifications identified by vendors of network equipment and software products. Qwest will have open discussions with the Government, identifying the possibility of benefit or risk to the Networkx infrastructure before deployment.

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Qwest will comprehensively test all components of potential security refreshment (enhancements) prior to deployment into the Network infrastructure, to ensure no negative impact to current operational status and compliance with Government policies, regulations, and applicable laws. Qwest will provide to Agencies supporting data identifying the impact of security refreshment to operational Network infrastructure.

Finally, [REDACTED] Qwest includes an interdisciplinary approach with the use of “what-if” scenarios, piloting customized services, and ongoing participation in technology forums and standards bodies to innovate and implement the latest in security trends and capabilities.

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

11.2 ENSURING EFFECTIVENESS OF CONTROLS

Qwest's approach to ensuring the effectiveness of our management, operational, and technical security controls, as defined in NIST SP 800-14 pertaining to the integrity, confidentiality, and availability of Government information and data, includes a broad set of regular audit and assessment activities, conducted by both internal and external parties, as well as formal compliance management processes to ensure all findings of such assessment activities are addressed in a timely manner.

Qwest's approach to ensuring the effectiveness of our management, technical, and operational security controls includes a broad set of regular audit and assessment activities, conducted by both internal and external parties, as well as formal compliance management processes and ongoing research and development of new controls and technologies. Qwest

discussed some of these processes for developing new and improved security-related processes in Section 14.0 of this Networkx Security Plan.

Qwest will conduct security risk analyses, reviews, assessments and/or evaluations of Networkx services annually, throughout the life of the contract, as required. 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 Networkx services.

Without this process, the security of Networkx may degrade over time as technology changes, systems evolve, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

In addition to these ongoing assessment activities, Qwest engages in ongoing Research and Development (R&D) in security-related products, functions and services. This R&D within our Technology Management organization is led by the Chief Technology Officer, and projects are performed by dedicated security engineers. Qwest also supports extensive work in industry forums and standards-setting groups by both the CTO organization and Qwest's dedicated Risk Management InfoSec organization. Together, these activities ensure both the effectiveness and innovative nature of Qwest's security program.

12.0 NON-DOMESTIC SERVICE SECURITY MANAGEMENT

As a provider of communication services globally, it is critical to our business to have strong relationships with other providers whose performance and quality standards are maintained and adhered to at the highest level.

[REDACTED]

In addition, a team of dedicated professionals from Qwest Operations monitors SLA performance of our non-domestic vendors around the clock, and are able to act quickly to any outages or other factors that may affect

Qwest's services, and administer penalties when service metrics are not met. Our non-domestic vendors monitor their core networks 24x7x365, and are held to the highest standards of quality and reliability in serving Agencies.

Within 30 minutes of determining a service-affecting or fraud-related event, the Qwest Network CPO will report verbally to the GSA Network PMO and the Contracting Officer (CO) any unusual or suspicious outage, blockage, or tampering that may indicate that users of services are being denied service, or services are being compromised.

Qwest's Network Operations Center has primary responsibility for managing all reported troubles, security violations and fraud incidents that affect the Qwest network and any network being used by Qwest to supply services to Agencies. When a problem is reported to the NOC or detected by the NOC, and it is determined that the problem may be caused by a domestic/non-domestic service provider, the NOC will notify the service provider that a problem has been reported. Per our service agreements, the service provider must provide an update to the Qwest NOC within [REDACTED] from initial notification and provide updates [REDACTED]. Escalations will begin [REDACTED] after the initial notification has been made or based on the severity of the problem. Escalations to the service provider's next level of management will occur until the VP level is reached (usually the 5th level of escalation). After the problem is resolved, a full report outlined the reasons for the problem is to be delivered to Qwest [REDACTED].

Our security related SLAs address time of notification for security breaches, time of notification for suspected fraudulent use of services, frequency of status updates and reporting.

13.0 FRAUD PREVENTION MANAGEMENT

Qwest's current, state-of-the-art fraud detection system includes regular assessments and reviews for effectiveness that include methods to continually improve its technologies and processes. Qwest Network Fraud Operations Center owns the responsibility of Fraud Prevention Management as a function within Qwest's integrated enterprise Risk Management Program.

13.1 PROACTIVE AND PREVENTATIVE APPROACH

The Qwest fraud management program regularly assesses current strategies, fraud system performance, and fraud prevention strategies, related not only to the Qwest network, but also to trends that emerge within the industry. This assessment allows Qwest to implement potential safeguards to reduce fraud exposure to Agencies. Qwest participates in various industry fraud organizations [REDACTED] [REDACTED] to assimilate current threats, trends, methodologies, and remedies. Qwest will contact Agencies to alert them of potential fraud, and assist them with up-to-date strategies in defending against fraud. Qwest also provides relevant fraud information on our website, www.qwest.com.

The Network Fraud Group's goal is to react quickly to a fraud situation to minimize any exposure and losses that may result from toll fraud. Qwest's integrated Network Security Team will alert the GSA and Agencies to the new trends in telecommunications fraud, and will provide them with up-to-date strategies for protection against toll fraud.

Qwest uses a state-of-the-art fraud detection system [REDACTED] [REDACTED]. The fraud center proactively and aggressively monitors the Qwest network 24x7x365, to ensure Agencies receive the

highest level of service. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. These preventative steps are implemented to protect Agencies against potential abuse.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Qwest will work with an Agency to advise and resolve any issues.

13.1.1 Calling Card Fraud Detection

Qwest Calling Cards provided under the Networx contract will be monitored by Qwest's advanced fraud systems for potential fraudulent use, misuse, or abuse on a 24x7x365 basis [REDACTED]
[REDACTED]

[REDACTED] It is Qwest's goal to minimize the interruption of service related to the deactivation of a Calling Card due to fraud. Consequently, Qwest will generate a new card for the Agency as quickly as possible.

Qwest's detection parameters include many elements that may be an indicator of unauthorized usage such as international calling to known fraud

countries, long duration calls, multiple call attempts in a short period of time, and simultaneous usage of a card.

13.1.1.1 Calling Card Dialing Restrictions

At the request of GSA or an Agency, Qwest's Calling Cards can be restricted from certain types of use, such as not allowing international origination or international termination. These restrictions will minimize the potential for fraudulent abuse if the card is compromised.

13.1.1.2 Customer Notification

Qwest, at the direction of the GSA Networkx PMO, will establish special handling procedures in notifying the Agency of suspected fraudulent use.

[REDACTED]

13.1.2 Customer Premise Equipment Fraud

Qwest's integrated Security Team will assist and cooperate fully in efforts to prevent and correct unauthorized use by informing the GSA Networkx PMO or Agencies of suspected fraudulent use. Qwest's Networkx CPO will consult with Networkx Agencies regarding defensive measures the Agencies can use that may reduce their exposure to misuse or abuse associated with the operation of Agency-provided systems, equipment, facilities, or services that are interconnected with Qwest's services. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Qwest will provide fraud

services to the Government for all products and services that are interconnected to Qwest facilities. This includes voice services (one-plus, dedicated outbound, dedicated inbound, toll free, calling card, and VoIP).

[REDACTED]

[REDACTED]

[REDACTED] Qwest will partner with the necessary Government representatives to make recommendations on settings that may safeguard their premise equipment from being compromised by unauthorized callers. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Government may need to make necessary changes or corrections within their premise equipment to prevent fraud. Qwest will partner with the Government, to implement necessary network solutions that will minimize any fraud exposure.

Qwest regularly monitors network traffic in an effort to identify abnormal calling patterns that may indicate toll fraud. Qwest routinely contacts Agencies when suspected fraud is detected on Agency premise equipment, systems, facilities, or services that are interconnected with Qwest services.

This network monitoring by Qwest identifies abnormal calling patterns after the fraudulent calling has started. Qwest has been successful in identifying fraudulent calling, which helps to limit the Agency's exposure to fraud resulting from the operation of Agency-provided equipment, systems, facilities or services that are interconnected to Qwest's services. It is the responsibility of the Agency to secure all Agency-provided equipment.

The Networkx PMO, while attempting to identify, correct, and minimize the misuse or abuse of their services, can request that Qwest provide assistance by reconfiguring and restricting service that is provided by Qwest. At the PMO's request, Qwest will selectively block and take other actions in order to limit or prevent fraud resulting from the operation of Agency-provided systems, equipment, facilities, or services.

Qwest will, upon request, assist Agencies in the referral of all relevant information to State or Federal officials, for the purposes of prosecuting those individuals responsible for the abuse or misuse of an Agency's service.

13.1.2.1 Fraud Liability

[REDACTED]

14.0 IMPROVED SECURITY-RELATED PROCESSES AND TECHNOLOGIES

Through a variety of strategic vendor relationships and industry forums, Qwest is able to remain updated about improved security practices, processes, and technologies. Qwest engages in a proactive set of planning and management controls including security-related policy making, evaluations, and risk assessments, in order to make security practices a priority as new products, services, and other infrastructure components are contemplated and introduced. These activities encompass all the elements required to provide critical Networkx services, including the Qwest infrastructure, the OSS environment, and the Networkx services themselves. As detailed in Section 11.0 Security Refreshment, Qwest is committed to a multi-pronged approach to continuous improvement of our security posture and that of Agencies.

Driven by the Chief Technology Office, Qwest evaluates and tests new network security enhancements, products, and technologies identified by vendors, in partnership with risk management/information security, product management, engineering, and operations prior to incorporation into the Qwest network, to ensure there will be no negative impact. Qwest is committed to an open discussion with Agencies in order to identify relevant benefits and/or risks, before deployment of products, processes, and technologies into the Networx infrastructure.

Once approved by the GSA Networx PMO and Agencies, this Networx Security Plan will be updated and will become part of the certification process. However, if the process or technology cannot be implemented, Qwest will work with the GSA Networx PMO to find an alternative solution.

Qwest is an active participant in a wide range of standards groups to promote sound security practices, especially as new services such as VoIP emerge. Qwest participates in and seeks to continuously improve our security programs through data collection/metrics and analysis, including formal reviews of all CIRT activations to identify further opportunities for improving our information security posture.

By combining these processes for sound, rigorous engineering practices in implementing new products, features and services with our programs in vulnerability management and security assessments, Qwest will continue to demonstrate that sound security practices are not only a cornerstone of how we operate today, but will also demonstrate that Qwest is continuously improving as technology evolves and the threat climate changes.