Attachment 1 to Appendix 2

Risk Assessment Security Report for the 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
—	—	—	—
—	—	—	—
—	—	—	—

Introduction

The scope of Qwest's risk assessment includes all Networx related infrastructure and all Networx services, including the Qwest Networx OSS applications and data. Qwest will meet FISMA requirements based on the appropriate NIST security standards. FISMA requires Qwest to conduct a risk assessment based on NIST SP 800-26 and set baseline security access controls based on NIST SP 800-53/FIPS 200 to protect the integrity, confidentiality, and availability of the Qwest Control Networx Portal System used by GSA and the Agencies to interface with Qwest's OSS.

Specifically, Qwest will focus on the following key components of its [redacted] risk assessment methodology:

- Security vulnerabilities of all Networx services as they pertain to ensuring integrity, confidentiality, and availability of the services and Government information that may be stored or transported by such services
- Security vulnerabilities of the Qwest Control Qwest Control Networx Portal and OSS as they pertain to integrity, confidentiality, and availability of the Government information that may be stored and processed by the OSS.

The Security Control Selections summarized in table format in this attachment are based on an impact assessment that the loss of integrity, confidentiality, and availability would have on the OSS and Networx services. This analysis will provide Qwest the preliminary guidance on the implementation of baseline technical, operational, and management security controls on the Portal and OSS.

In accordance with FISMA/NIST guidance, and analysis of the RFP the Qwest Control Networx Portal and OSS Security Controls are initially rated as Moderate impact based on FIPS 199, as interpreted by Qwest. The FIPS 199 security control categories (high, moderate and low) are assessed and the

results are based on the impact adverse events would have on the Qwest Control Networx Portal and OSS mission and operations.

The initial impact assessment is preliminary in nature and represents the starting point in the security process. This assessment does not constitute the final security configuration. A collaborative effort between Qwest, the Designated Approving Authority and all stakeholders is required, after contract award, to define a comprehensive assessment of security controls.

The Security Controls in ***Figure A2.1-1*** are applied to the Qwest Control Networx Portal and OSS in accordance with Annex 2, to NIST Special Publication 800-53, titled Recommended Security Controls for Federal Information Systems. The Qwest assessment is based on the "moderate" baseline for security controls in support of FISMA compliance Certification and Accreditation activities.

Figure A2.1-1. FIPS 199 MODERATE IMPACT SECURITY CONTROLS

Control #	Control Name	[redacted]	Supplemental Guidance
AC-1	Access Control Policy And Procedures	[redacted]	The access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
AC-2	Account Management	[redacted]	Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. [redacted]

Control #	Control Name	[redacted]	Supplemental Guidance
		[redacted]	[redacted]
AC-3	Access Enforcement	[redacted]	Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling [redacted] If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 compliant.
AC-4	Information Flow Enforcement	[redacted]	Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).
AC-5	Separation Of Duties	[redacted]	[redacted]

Control #	Control Name	[redacted]	Supplemental Guidance
			[redacted]
AC-6	Least Privilege	[redacted]	
AC-7	Unsuccessful Login Attempts	[redacted]	
AC-8	System Use Notification	[redacted]	Privacy and security policies are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. For publicly accessible systems: (i) the system use information is available as opposed to displaying the information before granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control #	Control Name	[redacted]	Supplemental Guidance
AC-11	Session Lock	[redacted]	Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.
AC-12	Session Termination	[redacted]	None.
AC-13	Supervision And Review — Access Control	[redacted]	[redacted]
AC-14	Permitted Actions Without Identification Or Authentication	[redacted]	[redacted]
AC-17	Remote Access	[redacted]	Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. [redacted] NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control #	Control Name	[redacted]	Supplemental Guidance
AC-18	Wireless Access Restrictions	[redacted]	NIST Special Publication 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards.
AC-19	Access Control For Portable And Mobile Devices	[redacted]	Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to organizational networks without first meeting organizational security policies and procedures. Security policies and procedures might include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).
AC-20	Personally Owned Information Systems	[redacted]	[redacted]

Control #	Control Name	[redacted]	Supplemental Guidance
AT-1	Security Awareness And Training Policy And Procedures	[redacted]	The security awareness and training policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.
AT-2	Security Awareness	[redacted]	[redacted]
AT-3	Security Training	[redacted]	[redacted]
AT-4	Security Training Records	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
AU-1	Audit And Accountability Policy And Procedures	[redacted]	The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. [redacted] NIST Special Publication 800-12 provides guidance on security policies and procedures.
AU-2	Auditable Events	[redacted]	[redacted]
AU-3	Content Of Audit Records	[redacted]	Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.
AU-4	Audit Storage Capacity	[redacted]	None.
AU-5	Audit Processing	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
AU-6	Audit Monitoring, Analysis, And Reporting	[redacted]	None.
AU-7	Audit Reduction And Report Generation	[redacted]	Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.
AU-8	Time Stamps	[redacted]	Time stamps of audit records are generated using internal system clocks that are synchronized system wide.
AU-9	Protection Of Audit Information	[redacted]	None.
AU-11	Audit Retention	[redacted]	NIST Special Publication 800-61 provides guidance on computer security incident handling and audit log retention.
CA-1	Certification, Accreditation, And Security Assessment Policies And Procedures	[redacted]	The security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on processing security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.
CA-2	Security Assessments	[redacted]	This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually. NIST Special Publications 800-53A and 800-26 provide guidance on security control assessments.

Control #	Control Name	[redacted]	Supplemental Guidance
CA-3	Information System Connections	[redacted]	Since FIPS 199 security categorizations apply to individual information systems, the organization should carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations should also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on interconnecting information systems.
CA-4	Security Certification	[redacted]	A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is integrated into and spans the System Development Life Cycle (SDLC). NIST Special Publication 800-53A provides guidance on the assessment of security controls. NIST Special Publication 800-37 provides guidance on security certification and accreditation.
CA-5	Plan Of Action And Milestones	[redacted]	The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.
CA-6	Security Accreditation	[redacted]	OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems.

Control #	Control Name	[redacted]	Supplemental Guidance
CA-7	Continuous Monitoring	[redacted]	Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. [redacted] NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls.
CM-1	Configuration Management Policy And Procedures	[redacted]	The configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
CM-2	Baseline Configuration	[redacted]	The configuration of the information system is consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).
CM-3	Configuration Change Control	[redacted]	Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. [redacted]
CM-4	Monitoring Configuration Changes	[redacted]	[redacted]
CM-5	Access Restrictions For change	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
CM-6	Configuration Settings	[redacted]	NIST Special Publication 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.
CM-7	Least Functionality	[redacted]	Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).
CP-1	Contingency Planning Policy And Procedures	[redacted]	The contingency planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.
CP-2	Contingency Plan	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
CP-3	Contingency Training	[redacted]	None
CP-4	Contingency Plan Testing	[redacted]	There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises).
CP-5	Contingency Plan Update	[redacted]	Organizational changes include changes in mission, functions, or business processes supported by the information system. [redacted]
CP-6	Alternate Storage Sites	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
CP-7	Alternate Processing Sites		Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site.
CP-8	Telecommunic a-tions Services		In the event that the primary and/or alternate telecommunications services are provided by a wireline carrier, the organization should ensure that it requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).
CP-9	Information System Backup		The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control #	Control Name	[redacted]	Supplemental Guidance
CP-10	Information System Recovery And Reconstitution	[redacted]	Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.
IA-1	Identification And Authentication Policy And Procedures	[redacted]	The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73 and 800-76; and (ii) other applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
IA-2	User Identification And Authentication	[redacted]	Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low-impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Control #	Control Name	[redacted]	Supplemental Guidance
IA-3	Device Identification And Authentication	[redacted]	The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.
IA-4	Identifier Management	[redacted]	Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors.
IA-5	Authenticator Management	[redacted]	Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) proh bits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
IA-6	Authenticator Feedback	[redacted]	The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).

Control #	Control Name	[redacted]	Supplemental Guidance
IA-7	Cryptographic Module Authentication	[redacted]	None.
IR-1	Incident Response Policy And Procedures	[redacted]	The incident response policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-12 provides guidance on security policies and procedures.
IR-2	Incident Response Training	[redacted]	None.
IR-3	Incident Response Testing	[redacted]	None.
IR-4	Incident Handling	[redacted]	[redacted]
IR-5	Incident Monitoring	[redacted]	None.
IR-6	Incident Reporting	[redacted]	The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

Control #	Control Name	[redacted]	Supplemental Guidance
IR-7	Incident Response Assistance	[redacted]	Possible implementations of incident support resources in an organization include a help desk or an assistance group and access to forensics services, when required.
MA-1	System Maintenance Policy And Procedures	[redacted]	The information system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
MA-2	Periodic Maintenance	[redacted]	Appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly.
MA-3	Maintenance Tools	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
MA-4	Remote Maintenance	[redacted]	[redacted]
MA-5	Maintenance Personnel	[redacted]	Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.
MA-6	Timely Maintenance	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
MP-1	Media Protection Policy And Procedures	[redacted]	The media protection policy and procedures are consistent with applicable federal laws, directives, [redacted] NIST Special Publication 800-12 provides guidance on security policies and procedures.
MP-2	Media Access	[redacted]	None.
MP-3	Media Labeling	[redacted]	[redacted]
MP-4	Media Storage	[redacted]	[redacted]
MP-5	Media Transport	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
MP-6	Media Sanitization	[redacted]	Sanitization is the process used to remove information from digital media such that information recovery is not possible. Sanitization includes removing all labels, markings, and activity logs. Sanitization techniques, including degaussing and overwriting memory locations, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The National Security Agency maintains a listing of approved products at http://www.nsa.gov/ia/Government/mdg.cfm with degaussing capability. The product selected is appropriate for the type of media being degaussed. NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.
MP-7	Media Destruction And Disposal	[redacted]	[redacted]. Media destruction and disposal should be accomplished in an environmentally approved manner. The National Security Agency provides media destruction guidance at http://www.nsa.gov/ia/Government/mdg.cfm. The organization destroys information storage media when no longer needed in accordance with organization-approved methods and organizational policy and procedures. [redacted] NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.
PE-1	Physical And Environmental Protection Policy And Procedures	[redacted]	The physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control #	Control Name	[redacted]	Supplemental Guidance
PE-2	Physical Access Authorizations	[redacted]	[redacted]
PE-3	Physical Access Control	[redacted]	[redacted]
PE-5	Access Control For Display Medium	[redacted]	None.
PE-6	Monitoring Physical Access	[redacted]	[redacted]
PE-7	Visitor Control	[redacted]	Government contractors and others with permanent authorization credentials are not considered visitors.

Control #	Control Name	[redacted]	Supplemental Guidance
PE-8	Access Logs		None.
PE-9	Power Equipment And Power Cabling		None.
PE-10	Emergency Shutoff		None.
PE-11	Emergency Power		None.
PE-12	Emergency Lighting		None.
PE-13	Fire Protection		Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control #	Control Name	[redacted]	Supplemental Guidance
PE-14	Temperature And Humidity Controls	[redacted]	None.
PE-15	Water Damage Protection	[redacted]	None.
PE-16	Delivery And Removal	[redacted]	[redacted]
PE-17	Alternate Work Site	[redacted]	NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications. The organization provides a means for employees to communicate with information system security staff in case of security problems.
PL-1	Security Planning Policy And Procedures	[redacted]	The security planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security planning policy can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.
PL-2	System Security Plan	[redacted]	NIST Special Publication 800-18 provides guidance on security planning.

Control #	Control Name	[redacted]	Supplemental Guidance
PL-3	System Security Plan Update	[redacted]	[redacted]
PL-4	Rules Of Behavior	[redacted]	Electronic signatures are acceptable for use in acknowledging rules of behavior. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.
PL-5	Privacy Impact Assessment	[redacted]	OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.
PS-1	Personnel Security Policy And Procedures	[redacted]	The personnel security policy and procedures are consistent with applicable federal laws, directives, [redacted] NIST Special Publication 800-12 provides guidance on security policies and procedures.
PS-2	Position Categorization	[redacted]	Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.
PS-3	Personnel Screening	[redacted]	Screening is consistent with: (i) 5 CFR 731.106(a); (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned position.

Control #	Control Name	[redacted]	Supplemental Guidance
PS-4	Personnel Termination	[redacted]	None.
PS-5	Personnel Transfer	[redacted]	None.
PS-6	Access Agreements	[redacted]	None.
PS-7	Third-Party Personnel Security	[redacted]	[redacted] NIST Special Publication 800-35 provides guidance on information technology security services.
PS-8	Personnel Sanctions	[redacted]	The sanctions process is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The sanctions process are included as part of the general personnel policies and procedures for the organization.

Control #	Control Name	[redacted]	Supplemental Guidance
RA-1	Risk Assessment Policy And Procedures	[redacted]	The risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.
RA-2	Security Categorization	[redacted]	NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. [redacted]
RA-3	Risk Assessment	[redacted]	Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.
RA-4	Risk Assessment Update	[redacted]	[redacted]. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.

Control #	Control Name	[redacted]	Supplemental Guidance
RA-5	Vulnerability Scanning	[redacted]	[redacted] NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 provides guidance on handling security patches.
SA-1	System And Services Acquisition Policy And Procedures	[redacted]	[redacted] NIST Special Publication 800-12 provides guidance on security policies and procedures.
SA-2	Allocation Of Resources	[redacted]	[redacted] NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.
SA-3	Life Cycle Support	[redacted]	NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Control #	Control Name	[redacted]	Supplemental Guidance
SA-4	Acquisitions	[redacted]	The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements for information systems categorized in accordance with FIPS 199. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. Use of Tested, Evaluated, and Validated Products NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products. Configuration Settings and Implementation Guidance The information system required documentation includes security configuration settings and security implementation guidance. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.
SA-5	Information System Documentation	[redacted]	Administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) optimizing the system's security features. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control #	Control Name	[redacted]	Supplemental Guidance
SA-6	Software Usage Restrictions	[redacted]	[redacted]
SA-7	User Installed Software	[redacted]	If provided the necessary privileges, users have the ability to download and install software. [redacted]
SA-8	Security Design Principles	[redacted]	NIST Special Publication 800-27 provides guidance on engineering principles for information system security.
SA-9	Outsourced Information System Services	[redacted]	Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced information system services documentation includes Government, service provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.

Control #	Control Name	[redacted]	Supplemental Guidance
SA-11	Developer Security Testing	[redacted]	Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.
SC-1	System And Communications Protection Policy And Procedures	[redacted]	The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
SC-2	Application Partitioning	[redacted]	The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.
SC-4	Information Remnants	[redacted]	Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.
SC-5	Denial Of Service Protection	[redacted]	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control #	Control Name	[redacted]	Supplemental Guidance
SC-6	Resource Priority	[redacted]	Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.
SC-7	Boundary Protection	[redacted]	Any connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.
SC-8	Transmission Integrity	[redacted]	The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distr bution Systems.
SC-9	Transmission Confidentiality	[redacted]	The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distr bution Systems.
SC-10	Network Disconnect	[redacted]	None.
SC-12	Cryptographic Key Establishment And Management	[redacted]	NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
SC-13	Use Of Validated Cryptography	[redacted]	NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
SC-14	Public Access Protections	[redacted]	None.

Control #	Control Name	[redacted]	Supplemental Guidance
SC-15	Collaborative Computing	[redacted]	None.
SC-17	Public Key Infrastructure Certificates	[redacted]	Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
SC-18	Mobile Code	[redacted]	Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: http://iase.disa.mil/mcp/index.html.
SC-19	Voice Over Internet Protocol	[redacted]	NIST Special Publication 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.
SI-1	System And Information Integrity Policy And Procedures	[redacted]	The system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control #	Control Name	[redacted]	Supplemental Guidance
SI-2	Flaw Remediation	[redacted]	[redacted]
SI-3	Malicious Code Protection	[redacted]	[redacted]
SI-4	Intrusion Detection Tools And Techniques	[redacted]	Intrusion detection and information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, virus protection software, log monitoring software, network forensic analysis tools).

Control #	Control Name	[redacted]	Supplemental Guidance
SI-5	Security Alerts And Advisories	[redacted]	[redacted]
SI-6	Security Functionality Verification	[redacted]	None.
SI-8	Spam And Spyware Protection	[redacted]	[redacted]
SI-9	Information Input Restrictions	[redacted]	Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control #	Control Name	[redacted]	Supplemental Guidance
SI-10	Information Input Accuracy, Completeness, And Validity	[redacted]	Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, and validity of information inputs should be guided by organizational policy and operational requirements.
SI-11	Error Handling	[redacted]	The structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.
SI-12	Information Output Handling And Retention	[redacted]	None.