
# CONNECT Reference System (CRS)

# Access Control Policy & Procedure

**Version 1.0**

**Release 2.1**

**3 November 2009**

## REVISION HISTORY

| REVISION | DATE | DESCRIPTION |
|---|---|---|
| 1.0 | 3 November 09 | Initial Release. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# TABLE OF CONTENTS

## LIST OF TABLES

## 1.0 Executive Summary

The CONNECT Reference System (CRS) simulates the secure transfer of health information between two agencies. The CONNECT gateway will provide a test platform other agencies can utilize to test their implementation of the CONNECT gateway without risking critical operational data or systems.

The overall goal of the CRS Access Control Policy and Procedure is to protect the Confidentiality, Integrity, and Availability of the CONNECT Reference system and its information by standardizing the NIST SP 800-53 AC family of controls for the CRS.

## 1.1 SECURITY CLASSIFICATION

The CRS has an overall system security categorization of MODERATE.

## 2.0 SYSTEM IDENTIFICATION

## 2.1 SYSTEM NAME / TITLE

| System Identifier | Response Data |
|---|---|
| Official System Name: | CONNECT Reference System |
| System Acronym: | CRS |
| System of Records (SOR): | N/A |
| Financial Management Investment Board (FMIB) Number: | 009-90-03-00-01-0004-00 |
| Select one System Type from the following: - GSS, GSS sub-system, MA or MA individual application | Major Application |

**SECTIONS 2.2 THROUGH 2.4 DELETED FOR PUBLIC VIEWING**

## 2.5 SYSTEM OPERATIONAL STATUS

| System Operational Status | Response Data |
|---|---|
| Select one System Operational Status from the following: New, Operational, or Undergoing a Major Modification. | New |

**SECTION 2.6 DELETED FOR PUBLIC VIEWING**

## 2.7 REFERENCES

- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors
- FIPS 140-2 Security Requirements for Cryptographic Modules
- OMB Memorandum 06-16 Protection of Sensitive Agency Information
- NIST 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST 800-28, Guidelines on Active Content and Mobile Code
- NIST 800-36, Guide to Selecting Information Technology Security Products
- NIST 800-41, Guidelines on Firewalls and Firewall Policy
- NIST 800-44, Guidelines on Securing Public Web Servers
- NIST 800-53rev2, Recommended Security Controls for Federal Information Systems
- NIST 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NIST 800-73, DRAFT Interfaces for Personal Identity Verification (4 Parts)
- NIST 800-76, Biometric Data Specification for Personal Identity Verification
- NIST 800-77, Guide to IPsec VPNs
- NIST 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- NIST 800-81, Secure Domain Name System (DNS) Deployment Guide
- NIST 800-83, Guide to Malware Incident Prevention and Handling
- NIST 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST 800-95, Guide to Secure Web Services
- NIST 800-100, Information Security Handbook: A Guide for Managers
- CONNECT Messaging Platform Service Interface Specification
- IETF RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- IETF RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

## 3.0 PURPOSE (AC-1)

The purpose of the CRS Access Control Policy and Procedure is to protect the Confidentiality, Integrity, and Availability of the CRS by implementing access controls to restrict logical access to the CRS within the accreditation boundary. The NIST SP 800-53 Access Control (AC) family of technical controls is the primary source for the structure and guideline for this document.

The layout of this document is intended to match the order of security controls employed by an information system of a Moderate security posture as defined by NIST SP 800-53. Each specific heading references its related NIST control to add clarity to the reader. Content that is specifically

related to a security control will be referenced appropriately in the preceding heading to maintain clearity.

This document and all policies and procedures for CRS are located in a centralized access controlled area:
https://wiki.agilexhealth.com/confluence/display/NHINCA/Home

## 3.1 SCOPE (AC-1)

The CRS Access Control Policy and Procedures are applicable to the Development Program Manager, Security Manger, Security Team, and Operations Team.

The CRS Access Control Policy and Procedure is provided by management to comply with and facilitate the implementation of controls within NIST SP 800-53 for a Moderate system security level. This document addresses each applicable control (Table 3.1-1) and references specific controls when necessary to provide clarity to the reader of the relationship of subjects to their respective controls.

**Table 3.1-1 Applicable AC Security Controls for Moderate Baseline Security**

| Access Control | | Enhancement |
|---|---|---|
| AC-1 | Access Control Policy and Procedures | AC-1 |
| AC-2 | Account Management | AC-2 (1) (2) (3) (4) |
| AC-3 | Access Enforcement | AC-3 (1) |
| AC-4 | Information Flow Enforcement | AC-4 |
| AC-5 | Separation of Duties | AC-5 |
| AC-6 | Least Privilege | AC-6 |
| AC-7 | Unsuccessful Login Attempts | AC-7 |
| AC-8 | System Use Notification | AC-8 |
| AC-9 | Previous Logon Notification | Not Applicable |
| AC-10 | Concurrent Session Control | Not Applicable |
| AC-11 | Session Lock | AC-11 |
| AC-12 | Session Termination | AC-12 |
| AC-13 | Supervision and Review—Access Control | AC-13 (1) |
| AC-14 | Permitted Actions without Identification or Authentication | AC-14 (1) |
| AC-15 | Automated Marking | Not Applicable |
| AC-16 | Automated Labeling | Not Applicable |
| AC-17 | Remote Access | AC-17 (1) (2) (3) (4) |
| AC-18 | Wireless Access Restrictions | AC-18 (1) |
| AC-19 | Access Control for Portable and Mobile Devices | AC-19 |
| AC-20 | Use of External Information Systems | AC-20 (1) |

## 3.2 ROLES AND RESPONSIBILITIES (AC-1)

Table 3.2-1 defines the roles and responsibilities of stakeholders involved with the CONNECT Reference System.

**Table 3.2-1 Roles and Responsibilities**

| Role | Responsibility |
|---|---|
| Development Program Manager | • The Development Program Manager has tactical-level responsibility for the IA program. In this role, the Development Program Manager should:<br>• Ensure that IA material developed is appropriate and timely for the intended audiences;<br>• Ensure that IA requirements are effectively deployed to reach the intended audience;<br>• Ensure that users and managers have an effective way to provide feedback on the IA material and its presentation;<br>• Ensure that IA material is reviewed periodically and updated when necessary |
| Security Manager (SM) | The SM is responsible for complying with IT security IA requirements established for their users. Managers should:<br>• Work with the Development Program Manager to meet shared responsibilities<br>• Serve in the role of system owner and/or data owner, where applicable<br>• Ensure that all users (including contractors) of their systems (i.e., genera complying with IA requirements<br>• Ensure that users (including contractors) understand specific rules of each system and application they use<br>• Separates sensitive duties to preclude any one individual from gaining the opportunity to adversely affect the CRS<br>• Verifies that the Development Program Manager has defined procedural checks and balances for personnel security and enforces these controls so accountability is established and security violations are detectable<br>• The SM establishes a process to ensure access privileges are revoked and immediately ceased prior to notifying those individuals whose employment status changes, such as being separated for adverse reasons (e.g., transfer, resignation, retirement, change of job description, etc.) |

| Role | Responsibility |
|---|---|
| | • All of the responsibilities in this policy apply equally to services performed by contractor and subcontractor personnel |
| Security Team | The Security Team is responsible for complying with IT security IA requirements as directed by the Security Team. The Security Team is responsible for:<br>• Enforcing IT security IA requirements established for their users Information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts<br>• Reviewing information system accounts on a monthly basis<br>• Enforcing assigned authorizations for controlling access to the system in accordance with applicable policy<br>• Enforcing assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy<br>• Enforces separation of duties through assigned access authorizations<br>• Enforcing the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks<br>• Enforces a limit of consecutive invalid access attempts by a user during a time period. The information system automatically locks the account/node for; delays next login prompt according to when the maximum number of unsuccessful attempts is exceeded<br>• Ensures an approved, system use notification message before granting system access informing potential users<br>• Ensures the system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon<br>• Ensures the system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon<br>• Ensures system automatically terminates a session after a predefined time of inactivity<br>• Ensures specific user actions that can be performed on the information system without identification or authentication<br>• Ensures remote access is monitored for all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access |

| Role | Responsibility |
|---|---|
| | method<br>• Restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information<br>• Defines specific user actions that can be performed on the information system without identification or authentication<br>• establishes usage restrictions, implementation guidance, documents, for portable and mobile devices<br>• Supports enforcement of the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks<br>• Ensures the information system uniquely identifies and authenticates users (or processes acting on behalf of users)<br>• Ensures the information system identifies and authenticates specific devices before establishing a connection<br>• Ensures for authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2 |
| Operations Team | Operations Team is responsible for implementing all account management functions, including:<br>• Implementing and maintaining IA configuration requirements<br>• Management of information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts<br>• Supporting enforcement of assigned authorizations for controlling access to the system in accordance with applicable policy |

### 3.3 COMPLIANCE AND DISSEMINATION (AC-1)

The CONNECT Reference System ensures identification, authentication and access control compliance by meeting the requirements established by NIST SP 800-53. The Program Development Manager provides the Account Management Policy and Procedure to address Access Control responsibilities and ensure that all users maintain an appropriate Access Control (AC) perspective. The Account Management Policies and Procedures to are disseminated to the appropriate members of the CONNECT Program team within the organization. The CONNECT Program is required to implement this Policy and Procedure. The Development Program Manager ensures the policies and procedures have appropriate baselines, and are controlled and disseminated to the CONNECT team in a centrally located area (https://wiki.agilexhealth.com/confluence/display/NHINCA/Home ) to ensure compliance.

This Policy and Procedure is compliant with applicable laws, directives, policies, regulations, standards, and guidance. The Development Program Manager is committed to implementation of

security controls. The Program Management Plan (PMP) describes the compliance requirements, management commitment, coordination among organizational entities, and compliance. The CRS Access Control Policy and Procedure is reviewed by responsible parties within the organization at least annually.

## 4.0 ACCOUNT MANAGEMENT (AC-2)

The CONNECT Program team manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The CRS Systems Administrator (SA) reviews information system accounts at least monthly. Due its operational nature, the only CRS accounts are Administrative and System. All other accounts are disabled per the applicable OS hardening guide.

## 4.1 OPERATING SYSTEMS

### 4.1.1 Solaris

#### 4.1.1.1 Account Creation/Modification

Solaris login accounts are created locally on the Solaris Operating System. All accounts generated are at first given a generic password In Accordance With (IAW) control IA-5 of the Identification and Authentication Policy and Procedure and will be changed upon initial login. No temporary or emergency accounts are authorized unless approved by Management for the purpose of restoring services by an authorized, cleared vendor or consultant (CRS Personnel Security P&P) and only for the duration of maintanence.

#### 4.1.1.2 Account Deactivation – Termination

System and Security Administrator account deactivation occurs through the Solaris Operating System once an exit checklist notification is received.

#### 4.1.1.3 Account Deactivation – Inactivity

If an Administrator does not login to the server for 45 days, the account is automatically suspended. Inactive accounts beyond 45 days are disabled by the system administrator.

### 4.1.2 Windows 2003, XP

#### 4.1.2.1 Account Creation/Modification

Windows login accounts are created locally on the Windows server. All accounts generated are at first given a generic password IAW with control IA-5 of the Identification and Authentication Policy and Procedure which is changed upon initial login. No temporary or emergency accounts are authorized unless approved by Management for the purpose of restoring services by an authorized, cleared vendor or consultant (CRS Personnel Security P&P) and only for the duration of maintanence. Only administrative accounts are authorized.

#### 4.1.2.2 Account Deactivation – Termination

System and Security administrator account deactivation occurs through the Windows Operating System once an exit checklist notification is received.

#### 4.1.2.3 Account Deactivation – Inactivity

If a user does not login to the workstation for 45 days, the account is automatically disabled. Inactive accounts are disabled by the system administrator.

### 4.1.3 CONNECT Application

The CONNECT Application does not provide user account access. Access to information between CONNECT Gateways is controlled by x.509 digital signature between exchanging entities. A Certificate Authority (CA) has not been identified for this release 2.1 of CRS. Therefore, agencies will manually exchange and maintain valid certificates locally in their controlled certificate repository while a CA is established. The CRS is never intended to handle real PHI; however, the distinction must be made here as reuse of CRS documentation by other organizations is inevitable. It is important that an appropriate key exchange and encryption mechanism (FIPS 140-2 compliant) is selected before implementation of a CONNECT gateway.

### 4.1.4 NETWORK DEVICES – Juniper Firewalls

#### 4.1.4.1 Account Creation/Modification

Juniper login accounts are created locally on the Juniper Device. All accounts generated are at first given a generic password, which is changed upon initial login. No temporary or emergency accounts are authorized. User accounts are not authorized.

#### 4.1.4.2 Account Deactivation – Termination

System and Security administrator account deactivation occurs through the Juniper Device once an exit checklist notification is received. User accounts are not authorized.

#### 4.1.4.3 Account Deactivation – Inactivity

If a user does not login to the device for 45 days, the account is automatically disabled. Inactive accounts are disabled by the system administrator.

## 5.0 Access Enforcement (AC-3)

The CRS restricts access to privileged functions within the system explicitly to authorized personnel.

## 5.1 OPERATING SYSTEMS

### 5.1.1 Solaris

Only authorized administrative users are allowed to access Solaris servers. Unprivileged users do not have access. Access is controlled by the local security policy of the operating system. The Solaris Operating System on the CRS has been hardened to the best industry standards using NIST and DISA Security Technical Implementation Guidelines (STIGs) and is documented in the CRS Solaris Hardening Guide.

### 5.1.2 Windows 2003

Only authorized administrative users are allowed to access the W2003 servers. Unprivileged users do not have access to the network infrastructure. Access is controlled by the local security policy of the operating system. The Windows Operating System on the CRS has been hardened to the best industry standards using NIST and DISA STIGs and is documented in the CRS Windows Hardening Guide.

### 5.1.3 CRS Application

The basis for authentication for National Health Information Network (NHIN) participants shall be X.509 certificates. All National Health Information Entity (NHIE) certificates for NHIN Trial Implementations will be issued by a common trusted certificate. All NHIE to NHIE messages must be digitally signed for the purpose of authentication and non-repudiation. A portion of the CRS is intended to test NHIE to NHIE messaging capabilities.

### 5.1.4 Network Devices – Juniper Firewall

Only authorized administrative users are allowed to access the Juniper Firewalls. General users do not have access to the network infrastructure.

## 6.0 Information Flow Enforcement (AC-4)

An agreement managed through a Data Use and Reciprocal Sharing Agreement (DURSA) or Interconnection Security Agreement (ISA) made between a CONNECT Gateway entity and the CRS governs the terms of use and ensures that no information will be shared without the information owner's consent. The agreement may also define Service Level Agreements, availability, information protection requirements, source and destination IP address and services required. The CRS Project Team does not currently maintain standard ISA documents but will review and comply with ISA documents authored by connected partners.

Boundary protection is enforced to allow or disallow access based on specially crafted rule sets on the firewall (see Table 7.3-1).

## 7.0 Separation of Duties (AC-5)

Due its operational nature, the only CRS accounts are Administrative and System. All other accounts are disabled per the applicable OS hardening guide. The CRS enforces separation of duties through system Access Control Lists (ACLs).

### 7.1 OPERATING SYSTEMS

#### 7.1.1 Solaris

Separation of duties through assigned access authorizations has been enforced for the Solaris system through local system ACLs.

#### 7.1.2 Windows 2003, XP

Separation of duties through assigned access authorizations has been enforced for the Windows system through local system ACLs.

### 7.2 CONNECT Application

The CONNECT Application inherits separation of duties from the Information System ACLs.

### 7.3 NETWORK DEVICES – Juniper Firewalls

Only authorized administrative users are allowed to make a direct connection to the Juniper Firewalls. Outside connections between authorized gateways are controlled at the firewall.

The table below identifies all of the currently public Web Service Description Language (WSDL) Interfaces supported by the CONNECT Gateway. This table includes the name of the WSDL, the services it handles, the port number, whether or not it is configurable, and whether or not it is SSL. All ports in the NHIN-CONNECT Gateway are configurable via either the Glassfish or Http Binding Component port settings.

**Table 7.3-1 Ports, Protocols and Services**

| WSDL | Services | Port | Configurable | SSL |
|---|---|---|---|---|
| AdapterAuditLogQuery | Audit Log Query | HttpDefaultPort | Yes | No |
| AdapterDocQuery | Document Query | HttpDefaultPort | Yes | No |
| AdapterDocRetrieve | Document Retrieve | HttpDefaultPort | Yes | No |
| AdapterReidentification | Subject Discovery – Reidentification | HttpDefaultPort | Yes | No |
| AdapterSubjectDiscovery | Subject Discovery – Announce and Revoke | HttpDefaultPort | Yes | No |
| AdapterSubscriptionManagement | HIEM - Subscribe and Unsubscribe | HttpDefaultPort | Yes | No |
| AdapterNotificationConsumer | HIEM – Notify | HttpDefaultPort | Yes | No |
| EntityAuditLogQuery | Audit Log Query | HttpDefaultPort | Yes | No |
| EntityDocQuery | Document Query | HttpDefaultPort | Yes | No |
| EntityDocRetreive | Document Retrieve | HttpDefaultPort | Yes | No |
| EntitySubjectDiscovery | Subject Discovery – Announce, Revoke, and Reidentification | HttpDefaultPort | Yes | No |
| EntitySubscriptionManagement | HIEM - Subscribe and Unsubscribe | HttpDefaultPort | Yes | No |
| EntityNotificationConsumer | HIEM – Notify | HttpDefaultPort | Yes | No |
| NhinAuditLogQuery | Audit Log Query | 8181 (Glassfish Https Port) | Yes | Yes |
| NhinSubjectDiscovery | Subject Discovery – Announce, Revoke, and Reidentification | 8181 (Glassfish Https Port) | Yes | Yes |
| NhinDocQuery | Document Query | 8181 (Glassfish Https Port) | Yes | Yes |
| NhinDocRetrieve | Document Retrieve | 8181 (Glassfish Https Port) | Yes | Yes |
| NhinSubscription | HIEM - Subscribe, Unsubscribe, and Notify | 8181 (Glassfish Https Port) | Yes | Yes |

## 8.0 Least Privilege (AC-6)

The CRS enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

## 8.1 OPERATING SYSTEMS

### 8.1.1 Solaris

Account privileges on the Solaris servers are granted based on user role and needs. Only administrators are authorized access on Solaris servers.

### 8.1.2 Windows 2003, XP

Account privileges on the Windows servers are granted based on user role and needs. Only administrators are authorized access on Windows servers.

Remote Management laptops are required to fully meet Federal Desktop Core Configuration (FDCC) standards.

## 8.2 CONNECT APPLICATION

The CONNECT Application inherits least privilage from the Information System ACLs.

## 8.3 NETWORK DEVICES – JUNIPER FIREWALL

Least privilege is enforced by restricted access. Only authorized administrative users are allowed to make a direct connection to the Juniper Firewalls. Network administrators, part of the Operations Team, require full access in order to perform maintenance and management duties.

## 9.0 Unsuccessful Login Attempts (AC-7)

Security Control Requirement: The information system enforces a limit of 3 consecutive invalid access attempts by a user during a 24 hour time period. The information system automatically locks the account/node for at least 15 minutes when the maximum number of unsuccessful attempts is exceeded.

## 9.1 OPERATING SYSTEMS

### 9.1.1 Solaris

Solaris servers lock out after 3 invalid login attempts.

### 9.1.2 Windows 2003, XP

Windows servers and workstations lock out after 3 invalid login attempts.

## 9.2 NETWORK DEVICES – JUNIPER FIREWALL

Firewalls lock out after 3 invalid login attempts.

## 10.0 System Use Notification (AC-8)

The CRS displays an approved, system use notification message banner before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording.

The following table is an example of the CRS warning banner employed on all servers and network equipment:

**Table 10.0-1 Example Warning Banner on CRS**

| |
|---|
| *** *WARNING* *WARNING* *WARNING* *** <br><br> Unauthorized access is a violation of U.S. Law, and may result in criminal or administrative penalties. Users shall not access other user's or system files without proper authority. Absence of access controls IS NOT authorization for access! NHIN-C information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized federal officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized federal officials. Use of this system constitutes consent to such monitoring. |

*** *WARNING* *WARNING* *WARNING* ***

Privacy Act notification. The Contractor shall ensure that the following banner is displayed on all NHIN-C systems that contain Privacy Act information operated by the contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

## 11.0 Session Lock (AC-11)

All CRS Servers and Network Equipment are configured to prevent further access to the system by initiating a session lock after 15 minutes of inactivity, and the session lock will remain in effect until the administrator, part of the Operations Team, reestablishes access using appropriate identification and authentication procedures.

Administrators are required to manually lock a session during daily operations and must log off at the end of the work day or when work is completed. The CRS Lab where servers are located is a controlled facility. Administrators are permitted to leave an active session unlocked only for the duration of admistrative activity. The 15 minute session lock prevents unauthorized access in the event an Administrator is unable to lock the session manually or forgets.

## 12.0 Session Termination (AC-12)

All CRS Servers and Network Equipment are configured to prevent further access to the system by initiating a session termination after 15 minutes of inactivity, and the session termination will remain in effect indefinitely.

The CONNECT Application inherits session termination from the Information System.

## 13.0 Supervision and Review (AC-13)

The Development Program Manager supervises and reviews the activities of Operations Team with respect to the enforcement and usage of CRS access controls at least monthly. Automated mechanisms (such as system logging functions) to facilitate the review of user activities on both Windows and Solaris Operating Systems are employed.

## 14.0 Permitted Actions without Identification and Authentication (AC-14)

The CRS does not permit user actions to be performed on the CRS without identification or authentication. The CRS does not permit actions to be performed without identification and authentication ever to accomplish mission objectives. All personnel must have been cleared throught CRS Personnel Security Policy and Procedure.

## 15.0 Remote Access (AC-17)

The CRS management has approved the use of remote access for administrative use only. Remote access will be provisioned and installed IAW NIST SP 800-77 Guide to IPsec VPNs.

## 16.0 Wireless Access Restrictions (AC-18)

Remote Management Labtops can connect remotely to the CRS over the encrypted IPSEC VPN provided by the VPN client. Remote Management laptops must be configured to not allow split tunneling.

## 17.0 Access Control for Portable and Mobile Devices (AC-19)

The only portable device permited for use on the CRS is the portable Remote Management Laptop. The Remote Management Laptop requires a unique user ID and password to authenticate the user to the local machine only. Access to the CRS is established by IPSEC VPN tunneling using the CRS Remote Administrator credentials. The CRS System Administrator accout may be used to perform remote maintainces following successfull IPSEC tunnelling. The Remote Management Laptop is not approved for any other use other than to perform authorized remote system maintainance to the CRS and will fall under the same accreditation requirements as the other components in the CRS accredidation boundary.

## 18.0 Use of External Information Systems (AC-20)

The use of external information systems to access the CRS is authorized only as a transport. The CRS Remote Management laptop will not be a member of any domain outside of the CRS to which it is assigned to maintain. The IPSEC tunnel from the CRS Remote Management Laptop will not be allowed to split tunnel and is required to meet all STIG requirements, and have the latest aniti-virus signatures, firewall rules, and intrusion prevention software. Monthly Nessus scans on the system will help prevent vulnerabilities from being introduced.